BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
LESLIE E. HURST (178432)
THOMAS J. O'REARDON II (247952)
ADAM M. BUCCI (327312)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
lhurst@bholaw.com
toreardon@bholaw.com
abucci@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW (*pro hac vice*)
ANTHONY L. PARKHILL (*pro hac vice*)
205 W. Randolph Street, #1630
Chicago, IL 60606
Tel: 312/621/2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION

SANDEEP KAPIL, GABRIELA GOMEZ and KIM SALLEN, and DANYELL SHIN on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

APPLE, INC.,

Defendant.

Lead Case No. 5:24-cv-09304-NW
Consolidated with 5:25-cv-05000-NW (Shin)

CONSOLIDATED FIRST AMENDED CLASS ACTION COMPLAINT

CLASS ACTION

District Judge Noël Wise
Courtroom 8, 4th Floor, San Jose Courthouse

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Sandeep Kapil, Gabriela Gomez, Kim Sallen, and Danyell Shin, on behalf of themselves and all others similarly situated, file their consolidated amended complaint against Apple, Inc. (Apple or Defendant), and in support thereof state:

INTRODUCTION

1. This case arises from Apple's deliberate misrepresentations about the safety and trustworthiness of its App Store. For years, Apple has used its App Store to bring consumers into the Apple ecosystem for the purpose of selling more Apple products. As part of its long-term branding effort, Apple has marketed its products and services as more secure and more trustworthy than any other consumer computer and smart phone hardware company, including the apps available through its App Store. By leveraging these promises and the goodwill created by its branding efforts, Apple has built a business model that depends not only on selling hardware such as iPhones and iPads but also on providing consumers with a curated selection of applications through the App Store. By maintaining exclusive control over the applications that may be downloaded on Apple devices, Apple has structured its ecosystem so that customers rely on Apple for the safety and reliability of the App Store. Apple has actively and extensively represented to consumers that apps on the App Store are thoroughly vetted, trustworthy, and secure. Apple has actively represented that its App Store apps which are used for cryptocurrency trading come from approved financial institutions and comply with all applicable laws.

2. These representations foster consumer trust, which, in turn, incentivize consumers to purchase Apple devices over competing brands and to regularly obtain apps through the App Store (another source of Apple profits). Apple's campaign to promote the safety and trustworthiness of its App Store directly contributes to increased sales of iPhones and other Apple products, as consumers reasonably believe that Apple's devices provide a safer and more secure user experience. Without this assurance of security, fewer consumers would be inclined to purchase Apple devices, as they might perceive other smartphones or tablets as equally secure or better suited to meet their needs. Consumers also would not download apps from developers they do not know or recognize absent Apple's representations that every app on the App Store has been vetted, is safe, and can be trusted.

3. Apple's assertions regarding the safety and legitimacy of App Store apps thus serve a dual purpose: enhancing the appeal of Apple's ecosystem while driving hardware sales. This is not merely a platform for app distribution but a cornerstone of Apple's competitive advantage in the smartphone and tablet market. Consequently, Apple profits not only from app sales or in-app purchases but also from free apps because Apple profits significantly from the added value that this perceived security brings to its devices, making the continued representation of app safety integral to Apple's market strategy and business growth.

4. Despite Apple's powerful marketing campaign, it has not spent the resources necessary to properly vet the apps, but instead allowed cybercriminals to exploit the image of trust Apple has established to steal money from Apple customers. Apple has chosen to reap the benefits of promoting its App Store as central to the benefits of Apple products while betraying those promises by providing substantial assistance that enabled cybercriminals to defraud consumers through the App Store. Without Apple's knowing participation and material support, the cybercriminals could not have accomplished these thefts.

5. Rather than take the preventative measures it promised to curb the rampant fraudulent conduct it knew about—including consumer complaints and public warnings that specific apps such as Digicoins and SolLuna were scams—or warn consumers of the risks of using the App Store, Apple chose to protect its decades-long marketing campaign. Apple knowingly assisted the fraud and allowed it to spread by using its powerful marketing capabilities to represent that the apps in its App Store were vetted, safe, secure, and reputable. Even though the App Store remains a significant vehicle for criminal activity, Apple continues to falsely advertise the App Store as a trusted platform central to the value of Apple products, while failing to fulfill its promises. Even when Apple customers report the crimes to Apple, it does little or nothing, including refusing to reimburse consumers for the money they lost through the fraudulent apps.

6. Apple has spent years assuring consumers that its App Store is uniquely safe and trustworthy. Its homepage and advertising campaigns lead with promises such as: "The apps you love. From a place you can trust." and "Privacy and security. Built into everything we do." Apple reinforces this message by declaring it is "Dedicated to trust and safety." These prominent

assurances, repeated across Apple's consumer-facing channels, cultivated the widespread belief that apps on the App Store are vetted, safe, and reliable. Apple's knowledge of fraud, coupled with its decision to conceal the truth and continue making these assurances, deepened consumer reliance while betraying the very trust it had cultivated.

7. Plaintiffs and Class members relied on Apple's extensive representations and ongoing and long-standing marketing campaign that its App Store is "a safe and trusted place" when they downloaded what purported to be trustworthy and legitimate digital asset trading applications, including Digicoins, SolLuna, Forex5, and Swiftcrypt. In reality, and unknown to Plaintiffs and Class members, these applications were "spoofing" programs created solely to steal money by obtaining users' account information and diverting Class members' assets to fraudsters. Not knowing this, and in reliance on Apple's express representations and longstanding marketing campaign that apps on the App Store were vetted, safe, legally compliant, Plaintiffs and Class members downloaded and used the apps, and saw what appeared to be legitimate trades and growing account balances. Eventually, their accounts in the apps were frozen and all the money they deposited was stolen in a cryptocurrency investment scam known as "pig butchering." Pig butchering is a form of confidence fraud in which victims are gradually lured into making larger investments in a seemingly legitimate platform before the perpetrators abscond with the funds—an approach that succeeds precisely because it exploits the trust Apple has cultivated.[1]

8. Apple's affirmative representations, and the overall impression created by its long-term campaign, conveyed that apps from its App Store could be trusted as safe and secure because of Apple's rigorous vetting and review process. Those representations were false and misleading. As a result of Apple's misrepresentations—and its failure to take appropriate corrective or remedial action—Apple has caused Plaintiffs and Class members to download apps created solely for fraudulent schemes and hence to suffer significant economic losses. Defendant's conduct violates the Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, *et seq*.; the Unfair

[1] *See* Office of Inspector General, *Pig Butchering Scams*, FDICOIG, available at https://www.fdicoig.gov/pig-butchering-scams (last visited May 28, 2025).

Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.; and the common law prohibition against negligent misrepresentations.

9. Through this class action, Plaintiffs seek to enjoin Apple's unlawful practices and to require that Apple compensate Plaintiffs and members of the Class for the losses they incurred as a result of Apple's misconduct.

THE PARTIES

10. Plaintiff Sandeep Kapil is a citizen of the State of California, the County of Riverside. As detailed more fully in paragraphs 90-97 below, a long-time Apple customer who purchased multiple iPhones and relied on Apple's marketing that the App Store was a safe and trusted place to download applications, Kapil downloaded the Digicoins app from the App Store believing it had been vetted and complied with Apple's guidelines for cryptocurrency trading apps. In reliance on Apple's assurances, he invested through Digicoins and ultimately lost more than $1.2 million in a pig-butchering scam that was enabled by Apple's false and misleading representations about the safety of App Store apps.

11. Plaintiff Gabriela Gomez is a citizen of the State of Texas, the County of El Paso. As detailed more fully in paragraphs 98-106 below, a long-time Apple customer who relied on Apple's assurances that the App Store was a safe and trustworthy platform, Gomez downloaded the Digicoins and SolLuna apps from the App Store believing they had been vetted and complied with Apple's guidelines. In reliance on Apple's representations, Gomez invested through those apps and lost approximately $72,000 in a pig-butchering scam, injuries made possible by Apple's false and misleading representations about the safety of App Store apps.

12. Plaintiff Kim Sallen is a citizen of the State of California, the County of San Diego. As detailed more fully in paragraphs 107-114 below, having used Apple products for nearly two decades, Sallen trusted Apple's long-term campaign that App Store apps are carefully vetted and safe. In reliance on that campaign, Sallen downloaded the Digicoins and Forex5 apps from the App Store, transferred funds, and ultimately lost approximately $120,000 when both apps proved to be fraudulent pig-butchering schemes—losses directly tied to Apple's false safety assurances.

13. Plaintiff Danyell Shin is a citizen of the State of Illinois, the County of Cook. As detailed more fully in paragraphs 115-122 below, Shin, a long-time Apple customer, trusted Apple's reputation and relied on its repeated assurances that the App Store was a safe, vetted marketplace. On that basis, Shin downloaded the Swiftcrypt app from the App Store and invested funds, ultimately losing approximately $80,000 in a pig-butchering scam that Apple enabled by falsely representing its App Store apps as secure and trustworthy

14. Defendant Apple, Inc. is California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014.

JURISDICTION AND VENUE

15. Jurisdiction is proper under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because, on information and belief, the proposed Class consists of 100 or more members; many of the members are citizens of states that are diverse from the state of Defendant's citizenship; and the amount in controversy exceeds $5,000,000, exclusive of costs and interest.

16. This Court may exercise personal jurisdiction over Apple, who has availed itself of the jurisdiction of this Court through acts and omissions, including but not limited to, having its principal place of business in this District, advertising its services in this District, selling products and services to consumers in this District, and by otherwise conducting business in this District; furthermore, various agreements between Apple and the Class select the Courts of this State as the proper forum for all disputes.

17. Venue is therefore proper in this forum pursuant to 28 U.S.C. § 1391(b), and further, as the Apple is located in this judicial district and/or a substantial part of the acts or omissions giving rise to the claims herein occurred in the same.

INTRADISTRICT ASSIGNMENT

18. Pursuant to Civil L.R. 3-2(c) and (e), assignment to the San Jose Division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in Santa Clara County, where Apple resides.

GENERAL ALLEGATIONS

A. The Scale and Reach of Apple's App Store

19. Apple is one of the largest mobile and tablet application providers in the world, through its universally known "App Store." It is one of the largest and most well-known corporations in the world with vast resources and goodwill developed through decades of careful branding. Apple reported over $391 billion in global revenue in 2024, with iPhone sales comprising approximately half of that amount. This reflects Apple's status as one of the most commercially dominant companies in the world.[2] Apple is one of the most valuable publicly traded companies in the world, with a market capitalization of approximately $2.86 trillion as of early 2025.[3]

20. Apple.com, Apple's one stop shop website which houses the app store, had approximately 728.78 million visits in July 2025 alone, making it the 49th most visited website worldwide and 35th in the United States.[4]

21. Apple has worked hard to be able to claim that it operates one of the most expansive and influential digital marketplaces in the world. The Apple App Store offers approximately 1.92 million apps available for download.

22. Each year, iOS users download more than 38 billion applications from the App Store, demonstrating the platform's deep integration into consumer behavior and daily digital life.[5]

23. In 2024 alone, Apple's App Store ecosystem facilitated over $1.3 trillion in billings and sales worldwide. This figure includes revenue from digital goods, services, and physical

---

[2] Hamza Tariq, *Apple's App Store Key Stats and Insights You Need to Consider in 2025*, Electronic Team, Inc. (Feb. 12, 2025), available at https://mac.eltima.com/app-store-stats/ (last visited Aug. 21, 2025).

[3] Tushar Thakur, *Apple Statistics 2025: Revenue, Devices & Services*, SQ Magazine (July 22, 2025), available at https://sqmagazine.co.uk/apple-statistics/ (last visited Aug. 21, 2025).

[4] SEMrush, *apple.com Web Traffic Statistics* (July 2025), available at https://www.semrush.com/website/apple.com/overview/ (last visited Aug. 21, 2025).

[5] *Apple App Store Statistics 2025: Key Insights and Trends*, TekRevol (May 6, 2025), available at https://www.tekrevol.com/blogs/apple-app-store-statistics/ (last visited Aug. 28, 2025).

products purchased through apps, reflecting the central role the App Store plays in global commerce.[6]

24. Apple's App Store receives over 813 million unique visitors each week, highlighting the sheer scale of its reach and the influence of its app distribution platform.[7]

B. Apple's Long-Term Trust & Safety Campaign

25. For many years, Apple has worked to build and promote a reputation of providing apps that are vetted, safe and can be trusted. Through a long-term, consistent, and widespread campaign, Apple has established and cultivated an image that its App Store is carefully curated with each app undergoing a rigorous review to ensure it meets Apple's safety and security standards. This campaign has successfully created and reinforced the general impression—and consumer belief—that apps on the App Store are safe and trustworthy by default.

26. The message of safe and secure apps begins with the structure of Apple's business model. Apple exercises exclusive control over app distribution on iOS devices, disallowing alternative app sources or "sideloading." For instance, Apple, in their 2021 article titled *Building a Trusted Ecosystem for Millions of Apps,* explained it prohibits sideloading because sideloading "would cripple the privacy and security protections that have made iPhone so secure, and expose users to serious security risks,"[8] reinforcing the long-term marketing message that Apple-approved apps on the App Store are safe and trustworthy.

---

[6] Apple, *The Global App Store and Its Growth* (June 2025), available at https://www.apple.com/newsroom/pdfs/2024-Apple-Global-Ecosystem-Report-June2025.pdf (last visited Aug. 21, 2025).

[7] *Id.*

[8] Apple, *Building a Trusted Ecosystem for Millions of Apps: A Threat Analysis of Sideloading* (Apple Inc. Oct. 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf (last visited Aug. 21, 2025).

1. Early Trust & Safety Messaging from Apple Executives

27. Apple's exclusive control over app distribution on Apple devices—and its prohibition of sideloading[9]—has long been marketed as a deliberate measure to protect users from dangerous, fraudulent, or malicious applications. From the outset, Apple represented itself as the gatekeeper ensuring that only safe, trustworthy apps reached consumers. At Apple's March 6, 2008, iPhone event—the first public unveiling of the App Store—Steve Jobs emphasized that while Apple and developers shared the goal of putting as many apps as possible into users' hands, Apple would refuse to distribute dangerous or untrustworthy apps:

> The developer and us have the same exact interest, which is to get as many apps out in front of as many iPhone users as possible. Now, will there be limitations? Of course. There are going to be some apps that we're not going to distribute. Porn, malicious apps, apps that invade your privacy. So, there will be some apps that we're going to say no to.[10]

[9] *Id.*

[10] *See Steve Jobs introduces the App Store – iPhone SDK Keynote*, YouTube (Mar. 13, 2008) (screenshot and quotation taken from keynote held Mar. 6, 2008), available at https://youtu.be/xo9cKe_Fch8?si=EqE6Cbp6fbzXYZEl (last visited Aug. 28, 2025); *see also* Ryan Block, *Live from Apple's iPhone SDK Press Conference*, Engadget (Mar. 6, 2008), available at https://www.engadget.com/2008-03-06-live-from-apples-iphone-press-conference.html (last visited Aug. 21, 2025).

28. Since its inception in 2007, the message of Apple only providing secure and vetted apps has been conveyed in public statements by Apple executives. In 2007, Jobs stated that Apple's mission for the App Store was to create "an advanced system which will offer developers broad access to natively program the iPhone's amazing software platform while at the same time protecting users from malicious programs."[11] In an interview in 2009, Apple marketing executive Phil Schiller represented to the publication Business Week that Apple had built an App Store that people could trust.[12]

29. Apple reiterated its approach to the App Store in 2010 when it released the first version of its App Store Review Guidelines, in which it stated "[i]f it sounds like we're control freaks, well, maybe it's because we're so committed to our users and making sure they have a quality experience with our products."[13]

2. Apple Nationwide Trust & Safety Advertising Campaigns

30. Apple's nationwide marketing campaigns have consistently reinforced this safety message. In 2009, Apple launched the nationwide *"There's an app for that"* campaign that was disseminated via television and the internet. The campaign was designed to convey not only the breadth of available applications but also their accessibility, reliability, and safety. By showcasing everyday problems—like checking the weather or finding directions—and resolving them effortlessly with apps from the App Store, Apple conveyed the message that every app offered was useful and trustworthy by design. This campaign laid the foundation for one of Apple's most memorable marketing slogans, which became synonymous with the iPhone and the App Store.

---

[11] Adam Engst, *Steve Jobs's iPhone SDK Letter*, TidBits (Oct. 17, 2007), available at https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/ (last visited Aug. 28, 2025).

[12] Jason Kincaid, *Phil Schiller Grants Interview About Apple's App Store, Claims Devs Actually Like Approval Process*, TechCrunch (Nov. 23, 2009), available at https://techcrunch.com/2009/11/23/phil-schiller-grants-interview-about-apples-app-store-claims-devs-actually-like-the-approval-process/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29&utm_content=Google+Reader (last visited Aug. 21, 2025).

[13] Leander Kahney, *Here's The Full Text of Apple's New App Store Guidelines*, Cult of Mac (Sept. 9, 2010), available at https://www.cultofmac.com/news/heres-the-full-text-of-apples-new-app-store-guidelines (last visited Aug. 21, 2025).

31. The *"There's an app for that"* campaign became one of Apple's most memorable and culturally pervasive marketing efforts. The phrase was repeated so widely that it entered everyday language, was parodied on *Sesame Street*, covered on *CBS Sunday Morning*, and ultimately trademarked by Apple. This cultural saturation reinforced the message that the App Store was not just expansive but also curated, safe, and reliable. By elevating the slogan into a household phrase, Apple deepened consumer reliance on its role as gatekeeper, encouraging consumers to equate Apple's approval of an app with trustworthiness and safety. The following are examples of how Apple has branded itself and the App Store as providing only reliable and safe apps.

32. For example, this trust and safety message was expressly conveyed in Apple's high-profile "If it's not an iPhone, it's not an iPhone" campaign in 2015—which aired nationally on television and online—that explicitly tied the safety and trustworthiness of Apple devices to the App Store ecosystem. In these advertisements, Apple contrasted the iPhone and its curated App Store with competitors' platforms, again messaging to consumers that only Apple could deliver a secure, thoroughly vetted library of applications:

> This is an iPhone. And it comes with something amazing. An AppStore with over one and a half million of the best apps available. That's over one and a half million ***hand-picked***, awe-inspiring, just-plain-surprising, who-knew-a-phone-could-do-that apps. If it's not an iPhone, it's not an iPhone.[14]

33. This 2015 advertising, along with other television, print, and digital media placements, continued to position the App Store as a "safe and trusted place" for consumers to download apps without fear of scams, malware, or fraud. These extensive advertisements are still accessible on YouTube for consumer consumption and are part of a long-running and highly successful branding effort.

3. Media Coverage and Executive Keynotes Amplifying Apple's Trust & Safety Message

34. To reinforce the overall trust and safety advertising campaign, Apple also generated extensive media coverage promoting its App Store review process and security measures. Company

[14] Apple, *iPhone – Amazing Apps*, YouTube (July 20, 2015), available at https://www.youtube.com/watch?v=IUtaogqn3rs (last visited Aug. 21, 2025).

executives have given interviews and delivered keynote speeches touting Apple's "stringent" app review standards, emphasizing that teams of experts review every app submission for malware, privacy compliance, and other security risks before the app is available in the App Store. Those, in turn, generate high volumes of "buzz media," third party news sources that further promote and disseminate Apple's messaging for it.

35. According to recent data from Altindex, Apple gets mentioned on X (formerly Twitter) approximately 3,774 times per day.[15] Media tracking service Meltwater has reported up to 239,000 social media mentions in a single day.[16]

36. In 2013, Wired, a major tech business and culture company that reaches more than 30 million people a month through their print and online mediums,[17] published an article on Wired.com which discussed how the App Store has "given consumers confidence that apps, no matter the developer, are trustworthy and secure."[18]

37. In 2021, Craig Federighi, Apple's Senior Vice President of Software Engineering, delivered the keynote address at Web Summit, a global technology conference attended by tens of thousands of industry professionals and consumers. The keynote, which has been viewed thousands of times on Web Summit's YouTube channel, underscored Apple's long-term narrative that the App Store is the critical safeguard protecting users from malicious software. Federighi described the threat landscape as "an industry motivated by profit," noting that cybercriminals use "social engineering" to trick users into downloading trojans that "suck up your personal data and help cyber

[15] AltIndex, *Apple (AAPL) – Twitter Mentions*, AltIndex (July 2025), available at https://altindex.com/ticker/aapl/twitter-mentions (last visited Aug. 21, 2025).

[16] TJ Kiely, *Brand Monitoring: How & Why You Should Keep Track of Your Brand Mentions* (July 23, 2025), available at https://www.meltwater.com/en/blog/brand-monitoring (last visited Aug. 21, 2025).

[17] Wired Press Center, *About*, available at https://www.wired.com/about/press/ (last visited Aug. 21, 2025).

[18] Christina Bonnington, *5 Years On, the App Store Has Forever Changed the Face of Software*, Wired (July 10, 2013), available at https://www.wired.com/2013/07/five-years-of-the-app-store/ (last visited Aug. 21, 2025).

criminals drain your bank account."[19] He characterized the App Store as the fail-safe complement to on-device protections, touting "human app review to limit people's exposure to scams in the first place, with real people evaluating every app to make sure that it worked as described."[20] These remarks have been widely reported and amplified by major news outlets, technology blogs, and consumer publications, reinforcing Apple's long-term, carefully cultivated image as the gatekeeper of safety in the digital marketplace. [21, 22]

4. Ubiquitous Trust & Safety Messaging Across Apple's Consumer-Facing Channels

38. Apple's long-term advertising campaign that the App Store is a "safe and trusted place" has never been confined to one medium or moment. Instead, Apple deliberately repeats the message across every consumer-facing channel—its website, App Store homepage, promotional materials, support pages, keynote events, and even search engine results—so that consumers cannot avoid the impression that apps from the App Store are safe, vetted, and trustworthy.

39. As part of this campaign, Apple saturates every consumer touchpoint—its website, App Store promotional materials, and product launch events—with repeated assurances that the App Store is uniquely curated to protect users from harm and fraud, and to provide the "safest place" to download apps. Apple's materials include phrases such as "Download with confidence", "The apps you love. From a place you can trust.", "For over a decade, the App Store has proved to be a safe and trusted place to discover and download apps.", and "Dedicated to trust and safety."[23] In the

---

[19] Craig Federighi, *Apple Keynote: Privacy and Security (Web Summit)*, YouTube (Nov. 2019), available at https://www.youtube.com/watch?v=f0Gum8UkyoI (last visited Aug. 21, 2025).

[20] *Id.*

[21] Amer Owaida, *1 Million Risky Apps Rejected or Removed from Apple's App Store in 2020*, *WeLiveSecurity* (May 12, 2021), available at https://www.welivesecurity.com/2021/05/12/1-million-risky-apps-rejected-apple-app-store-2020/ (last visited Aug. 21, 2025).

[22] Alan Friedman, *Morgan Stanley Bullish on Smartphones, See Android Doubling its Marketshare by Year End*, PhoneArena (Sept. 29, 2010), available at https://www.phonearena.com/news/sideloading-is-a-cybercriminals-best-friend-craig-federighi-web-summit-2021_id136189 (last visited Aug. 21, 2025).

[23] *See* Apple, *App Store*, https://www.apple.com/app-store/ (last visited Aug. 21, 2025). Apple has made these same representations on its App Store homepage prior to and throughout the class period, including: "The apps you love. From a place you can trust." "For over a decade, the App Store has proved to be a safe and trusted place to discover and download apps.", and "Dedicated to

context of financial and cryptocurrency-related apps, Apple has gone further, promising that such apps are "appropriately licensed" and from "approved financial institutions." Each of these assurances reinforced the campaign's core message: that Apple's vetting process shields consumers from dangerous or fraudulent apps. These promises deepened consumer reliance on the idea that downloading from the App Store was inherently safe. At the same time, by continuing to make such claims while approving and distributing fraudulent apps that Apple knew or should have known could not have satisfied its stated requirements or the trust-and-safety assurances it conveyed to the public—and by failing to act even after consumers warned Apple of the fraud—Apple betrayed the very trust it cultivates.

40. Apple repeated the same theme in 2021 when it published an article titled *Building a Trusted Ecosystem for Millions of Apps: The important role of App Store protections*. There, Apple told consumers:

> Nearly two million apps are available for users to download on the App Store, with thousands of apps added every week. Given the sheer scale of the App Store platform, ensuring iPhone security and safety was of critical importance to us from the start.... [W]e created the App Store, ***a trusted place where users can safely discover and download apps***. On the App Store, apps come from known developers who have agreed to follow our guidelines, and are securely distributed to users free from interference from third parties. We review every single app and each app update to evaluate whether they meet our high standards. This process, which we are constantly working to improve, is designed to protect our users by keeping malware, cybercriminals, and scammers out of the App Store.[24]

41. The following year, Apple reinforced this campaign message with another article, assuring consumers that it prevents "risky and untrustworthy apps and app updates from defrauding users." Apple boasted that "From App Review to Discovery Fraud, Apple's ongoing commitment

---

trust and safety." *See* Exhibit A attached (compendium of Apple's App Store homepage from 2020 to the present).

[24] Apple, *Building a Trusted Ecosystem for Millions of Apps: The important role of App Store protections* (June 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf (emphasis added) (last visited Aug. 21, 2025).

to protect users from fraudulent app activity demonstrates once again why independent, respected security experts have said the App Store is ***the safest place to find and download apps***."[25]

42. In 2024, Apple escalated the same campaign narrative in an article titled *App Store Stopped over $7 billion in potentially fraudulent transactions in four years.* That article declared: "Since launching the App Store in 2008, Apple has continued to invest in and develop industry-leading technologies designed to provide users with the safest and most secure experience for downloading apps ... Today, the App Store stands at the forefront of app distribution, setting the standard for security, reliability, and user experience."[26] Apple assured consumers that "[a]s digital threats have evolved in scope and complexity over the years, Apple has expanded its antifraud initiatives" claiming that "teams across Apple monitor and investigate fraudulent activity on the App Store, and utilize sophisticated tools and technologies to weed out bad actors and help strengthen the App Store ecosystem."[27]

43. In 2025, Apple once again repeated the same long-term campaign message. In an article published that year, Apple promised "the App Store's continued investment in fostering the most secure experience for users" and declared that "the App Store is a ***trusted destination for users to download*** their favorite apps and discover new ones."[28] Apple represented to consumers that it "employs a comprehensive approach to combating fraud on the App Store, with teams across the

[25] Apple, *App Store stopped nearly $1.5 billion in fraudulent transactions in 2021, Apple Newsroom* (June 1, 2022), available at https://www.apple.com/newsroom/2022/06/app-store-stopped-nearly-one-point-five-billion-in-fraudulent-transactions-in-2021/ (emphasis added) (last visited Aug. 22, 2025).

[26] Apple, *App Store stopped over $7 billion in potentially fraudulent transactions in four years*, *Apple Newsroom* (May 14, 2024), available at https://www.apple.com/newsroom/2024/05/app-store-stopped-over-7-billion-usd-in-potentially-fraudulent-transactions/ (emphasis added) (last visited Aug. 21, 2025).

[27] *Id.*

[28] Apple, *The App Store prevented more than $9 billion in fraudulent transactions over the last five years*, *Apple Newsroom* (May 25, 2025), available at https://www.apple.com/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/ (emphasis added) (last visited Aug. 21, 2025).

company working to detect, investigate, and prevent malicious activity before it can reach users."[29] Apple again assured users it "will continue to build on its commitment to provide users with ***the safest and most secure experience*** on the App Store."[30]

44. Apple also used its support pages to advance this same campaign. On its "App security overview" page on Apple.com, Apple repeated that it ensures apps are safe and secure:

> Apple provides layers of protection to help ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce that access from apps to user data is carefully mediated. These security controls provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps for iOS, iPadOS, and macOS—all without impacting system integrity. And users can access these apps on their Apple devices without undue fear of viruses, malware, or unauthorized attacks.[31]

45. On its support website, Apple once again assures users that the App Store "is a trusted place" that "protects users" by offering only safe and secure apps:

> The App Store is a trusted place where users can safely discover and download apps. On the App Store, apps come from identified developers who have agreed to follow Apple guidelines, and are securely distributed to users with cryptographic guarantees against modification. Every single app and each app update is reviewed to evaluate whether it meets requirements for privacy, security and safety. This process, which is being constantly improved, is designed to protect users by keeping malware, cybercriminals and scammers out of the App Store.[32]

46. Apple further states that unlike its competition it ensures all App Stores apps "come from identified developers and must pass automated and human review":

> Unlike other mobile platforms, iOS, iPadOS and visionOS don't allow users to install potentially malicious unsigned apps from websites or to run untrusted apps. Instead

---

[29] *Id.*

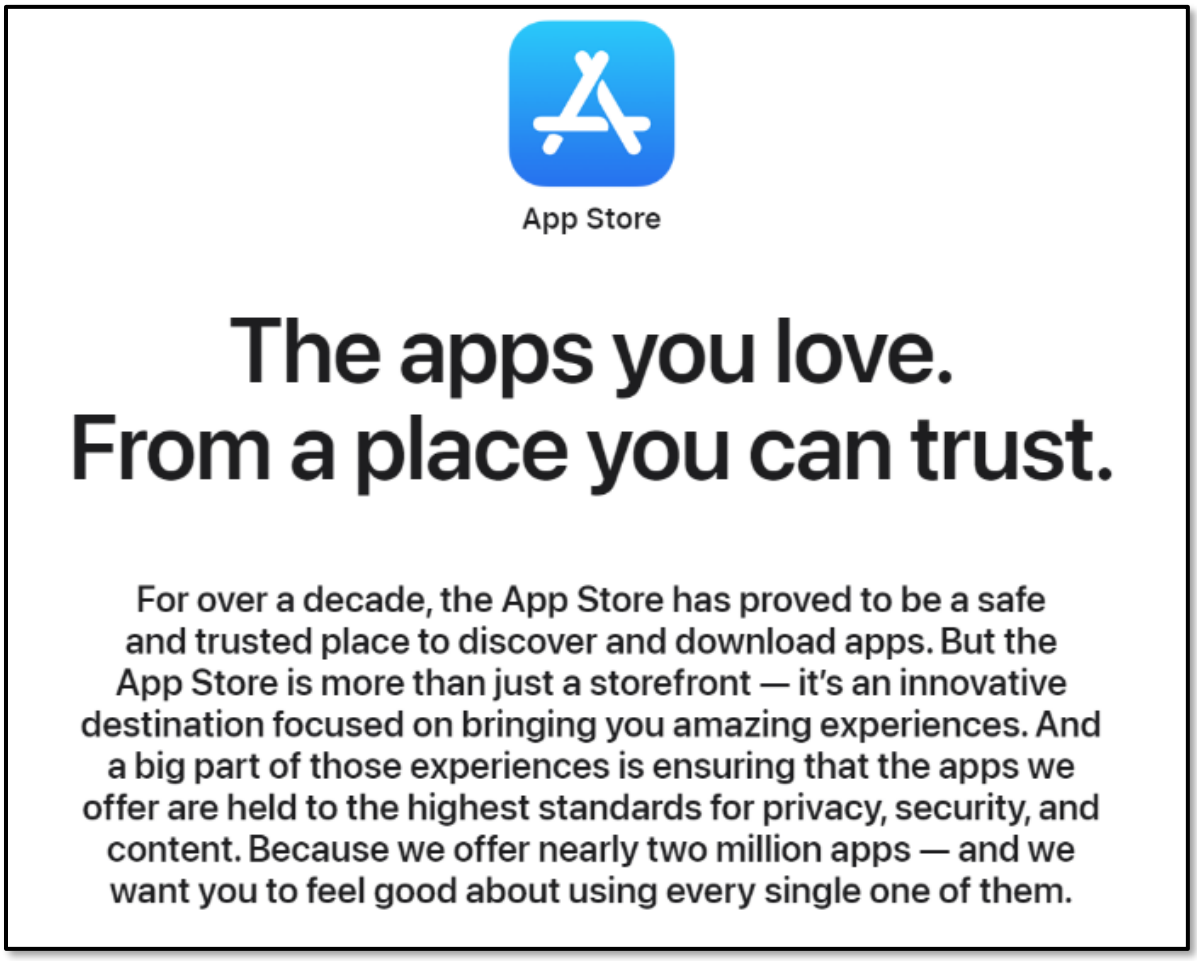
[30] *Id.* (emphasis added).

[31] Apple, *App Security Overview*, Apple Platform Security (Dec. 2024), available at https://support.apple.com/en-euro/guide/security/sec35dd877d0/web (last visited Aug. 27, 2025) (also available in *Apple Platform Security* (Dec. 2004), https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf).

[32] Apple, *About App Store security*, Apple Platform Security (Dec. 2024), available at https://support.apple.com/guide/security/about-app-store-security-secb8f887a15/ (last visited Aug. 27, 2025) (also available in *Apple Platform Security* (Dec. 2004), available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf).

> ... all apps must be downloaded from the App Store, where all apps come from identified developers and must pass automated and human review.[33]

47. The App Store homepage is Apple's most prominent consumer-facing platform and a centerpiece of its long-term campaign—a wall of security promises. Since at least September 2020, the first words a consumer sees boldly declare: "The apps you love. From a place you can trust."[34] This opening headline anchors the entire page in Apple's trust-and-safety messaging.



[33] Apple, *Intro to App Security for iOS, iPadOS and visionOS*, Apple Platform Security (Dec. 2024), available at https://support.apple.com/en-euro/guide/security/secf49cad4db/web (last visited Aug. 27, 2025) (also available in *Apple Platform Security* (Dec. 2004), https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf).

[34] Apple, *App Store* (homepage), Apple.com, available at https://www.apple.com/app-store/ (last visited Aug. 21, 2025). *See also* Exhibit A attached (compendium of Apple's App Store homepage from 2020 to the present).

48. And the message does not stop there. Throughout the homepage, Apple reinforces this trust and safety theme with statement after statement, repeated as the consumer scrolls. For example, scrolling down the homepage, among the specific assurances prominently displayed are:

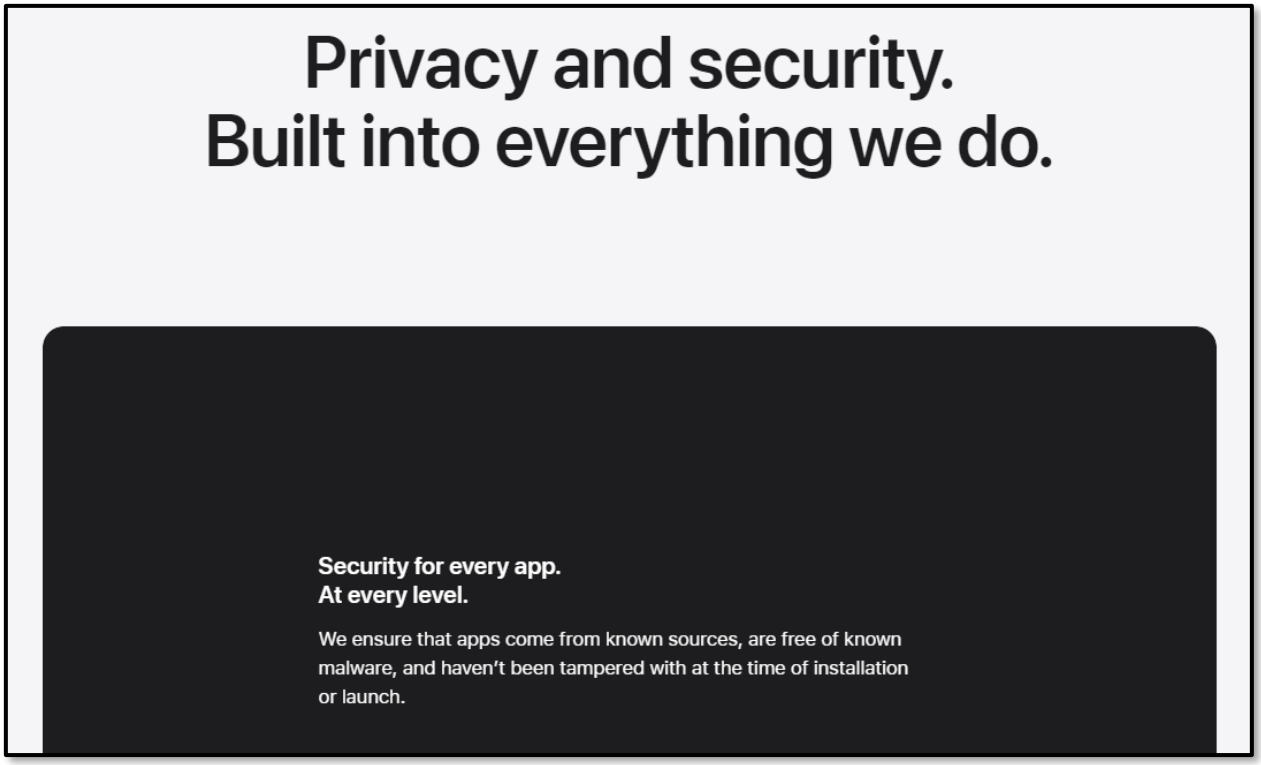
- "The apps you love. From a place you can trust."
- "For over a decade, the App Store has proved to be a safe and trusted place to discover and download apps."
- "Privacy and security. Built into everything we do."
- "Committed to security."
- "We conduct a thorough review to check that apps come from known sources, are free of known malware, and haven't been tampered with at the time of installation or launch."
- "100% of apps are automatically screened for known malware."
- "Dedicated to trust and safety."
- "Apps must adhere to our guidelines."
- "Every week, nearly 500 dedicated experts around the world review over 130k apps."
- "In 2024, more than 1.9 million submissions were rejected for reasons that include privacy violations and fraudulent activity."
- "Download with confidence."
- "Purchase safely and securely."
- "App Store purchases are safe and simple … Need a refund? Apple Support has your back."[35]

49. These statements are not buried in fine print; they are the central theme of Apple's homepage, presented in bold, repeated form to drive home the same point: that the App Store and its apps are safe, vetted, and trustworthy. Yet Apple approved and then allowed fraudulent apps to remain in the App Store—apps it knew or should have known could not have satisfied both its stated

[35] *Id.*

requirements and the trust-and-safety assurances it trumpeted to the public. In doing so, Apple not only deepened consumer reliance but also betrayed the very trust it had spent years cultivating.

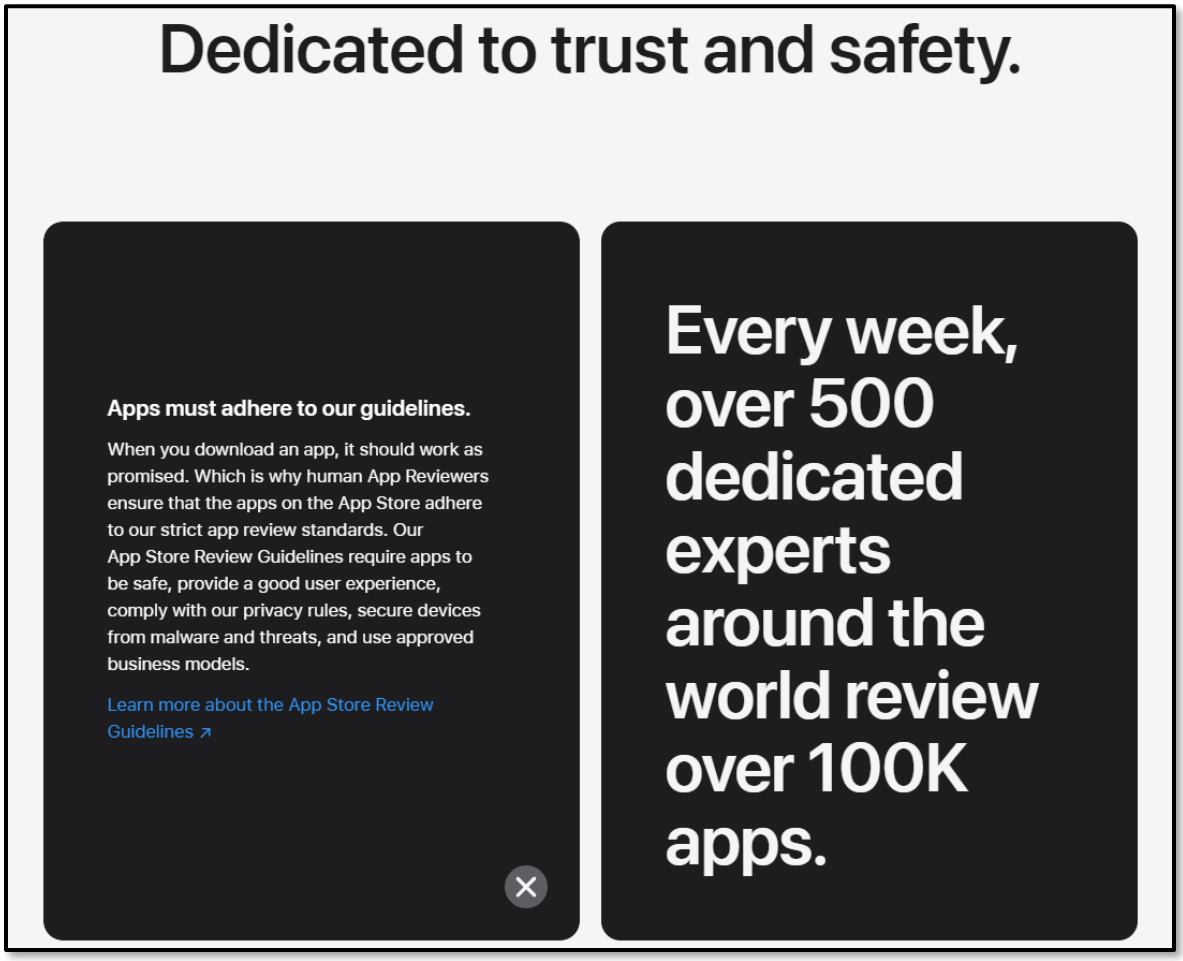
50. Screenshots from the homepage confirm this strategy. Since at least September 2020, Apple has prominently declared on its App Store homepage that the apps it makes available are "safe and trusted." Apple reinforces this campaign theme with statements such as "**Built into everything we do**," which convey not just that the App Store platform itself is secure, but that every app a consumer downloads can be trusted because Apple has rigorously reviewed and vetted it. These representations are part of Apple's long-term campaign to assure consumers that downloading apps from the App Store is inherently safe and reliable.[36]



51. Elsewhere on the same App Store homepage, Apple further proclaims it is "**Dedicated to trust and safety**," doubling down on the long-term message that safety is not peripheral but the very essence of the App Store.[37]

[36] *Id.*

[37] *Id.*



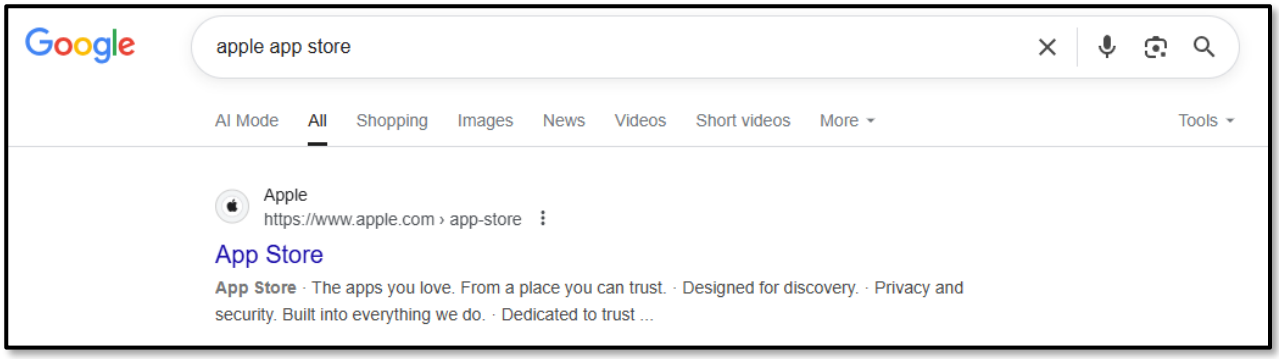
52. Apple extends this campaign by assuring consumers they can "**Download with confidence**," "**Purchase safely and securely**," and rely on AppleCare for support and refunds if anything goes wrong. These assurances reinforce Apple's overarching campaign theme: that consumers can trust the App Store as the exclusive safe source of apps for their devices.[38]

53. Apple deliberately structures its homepage to maximize the visibility of the trust and safety message for Google search results and search engine optimization (SEO) purposes. By placing its "safe and trusted" messaging at the top of the page, Apple ensures that even consumers who never click through see the assurances prominently displayed in Google results. For example, a search for "Apple App Store" returns a snippet including: "The apps you love. From a place you can trust." and "Dedicated to trust."[39]

---

[38] *Id.*

[39] Google search result for "Apple App Store," displaying Apple's App Store snippet text



54. Apple further designs its metadata and site structure to highlight these safety assurances, ensuring consumers consistently receive the impression that downloading apps from the App Store is uniquely safe and that Apple itself shields users from fraud and harm. These tactics reinforce Apple's long-term campaign to portray the App Store as the exclusive safe source of apps for its devices.

5. Apple's App Review Guidelines and Promises of Strict Vetting to Ensure Trust & Safety

55. Apple also emphasizes its complete control over the App Store. Before an app can be offered to consumers, Apple requires developers to submit the app for review, including its stated purpose, a working copy of the app, and supporting materials such as source code, user guides, and technical documentation. Apple then claims to vet this material and decides whether the app may be published on the App Store.[40]

56. These assurances were intended to convince consumers that the App Store was uniquely safe and secure. Apple's ongoing promises deepened consumer reliance on the belief that every app had been rigorously vetted and could be trusted. Yet Apple not only approved fraudulent applications designed to steal money, but knowingly allowed them to remain in the App Store long after red flags were raised by consumers. By continuing to repeat its trust-and-safety messaging

(showing that Apple's "safe and trusted" message appears directly in search results), available at https://www.google.com/search?q=apple+app+store (search conducted Aug. 21, 2025).

[40] *See, e.g.*, Apple, *App Review Guidelines*, Apple Developer, available at https://developer.apple.com/app-store/review/guidelines (last visited Aug. 21, 2025). *See also* Exhibit B attached (compendium of Apple's *App Review Guidelines* from 2018 to 2025).

while failing to act on clear warnings, Apple deepened consumer reliance and simultaneously betrayed the very trust it had cultivated.

57. As part of Apple's promise that apps from its App Store are vetted for safety and security, Apple represents and promises consumers that each app on the App Store has met its security standards. Apple reinforces this theme of trust by declaring: "***Customer trust is a cornerstone*** of the App ecosystem. Apps should never prey on users or attempt to rip off customers…"[41] Apple also states: ***"[t]he guiding principle*** of the App Store is simple—we want to provide a safe experience for users to get apps…"[42] These assurances are intended to foster consumer confidence in downloading and using apps from the App Store.

58. According to Apple and as stated in its *App Review Guidelines*, it achieves this "guiding principle" through "a highly curated App Store where every app is reviewed by experts." It further represents that it "scans each app for malware and other software that may impact user safety, security, and privacy," and that "apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected." Apple touts these measures as making its platforms "***the safest for consumers around the world***."[43]

59. Apple promises even stricter safeguards for financial apps, including cryptocurrency apps. According to Apple, such apps must come from established financial institutions, demonstrate compliance with licensing laws, and avoid misleading consumers:[44]

> 3.1.5 Cryptocurrencies:
>
> …
>
> (iii) Exchanges: Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered only in countries or regions where the app has appropriate licensing and permissions to provide a cryptocurrency exchange.
>
> (iv) Initial Coin Offerings: Apps facilitating Initial Coin Offerings ("ICOs"),

---

41 *Id*. (emphasis added).

42 *Id.* (emphasis added).

43 *Id.* (emphasis added).

44 *Id*.

> cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law.
>
> (v) Cryptocurrency apps may not offer currency for completing tasks, such as downloading other apps, encouraging other users to download, posting to social networks, etc.

60. Apple also represents that, as part of its vetting and review process, it takes extra vetting steps and precautions in the case of financial services apps:[45]

> Apps that provide services in highly regulated fields (such as banking and financial services, healthcare, gambling, legal cannabis use, and air travel) or that require sensitive user information should be submitted by a legal entity that provides the services, and not by an individual developer.

61. Apple further promises that if a fraudulent app is later discovered, it will be "immediately removed" from the App Store and users notified of the app's fraudulent activity:

> In a case where an app makes it into the App Store but is then later discovered to violate guidelines, Apple works with the developer to quickly resolve the issue. In dangerous cases, involving fraud and malicious activity, the app is immediately removed from the App Store and users who downloaded the app can be notified of the app's malicious behavior. [46]

62. Apple clearly conveys to consumers that its app review process is designed to guarantee trust and safety—emphasizing that every app is carefully vetted, reviewed by experts, and distributed through a secure and reliable App Store environment. In its June 2021 white paper, *Building a Trusted Ecosystem for Millions of Apps*, Apple declared that the "goal of App Review is to ensure that apps on the App Store are trustworthy."[47] In the *App Review Guidelines* Introduction, Apple likewise emphasized its "guiding principle" of providing "a safe experience for users to get

---

[45] *Id*.

[46] Apple, *About App Store Security,* Apple Platform Security (Dec 19, 2024), https://support.apple.com/guide/security/about-app-store-security-secb8f887a15/ (last visited Aug 21, 2025).

[47] Apple, *Building a Trusted Ecosystem for Millions of Apps – A Threat Analysis of the App Store's Security and Privacy Protections* (Apple Inc. June 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf (last visited Aug. 27, 2025).

apps," achieved through "a highly curated App Store where every app is reviewed by experts" and by scanning "each app for malware and other software that may impact user safety, security, and privacy."[48] Apple echoes these same assurances on its public-facing *App Review* webpage, which prominently states: "We review all apps, app updates, app bundles, in-app purchases, and in-app events submitted to App Store Connect to help provide a safe and trusted experience for users."[49]

C. The Reality: Apple Approved, Permits, and Assists the Fraudulent Apps

63. In practice, however, Apple approved and then allowed fraudulent financial and cryptocurrency apps to remain available on the App Store—apps that Apple knew or should have known could not have satisfied its stated requirements or the trust-and-safety assurances it conveyed to consumers. Apple's refusal to remove these apps even after being warned by users directly contradicted its promises of heightened safeguards. In doing so, Apple reinforced reliance on its long-term campaign while betraying the very trust it claimed to protect.

64. As with any long-term branding campaign, Apple's repeated promises have entered the collective consciousness of consumers, creating a widespread belief that apps on the App Store are safe and trustworthy—even among those who may not recall the specific representations.

65. Apple has consistently made these representations of safety and security in the applications offered in the App Store for nearly two decades as a focal point of widespread advertising and marketing.

66. Despite this long-running campaign and message, Apple approved apps such as Digicoins, SolLuna, Forex5, and Swiftcrypt—apps that had no proper licensing, no credible developer identity, and existed solely to steal funds. These apps could not have met Apple's stated requirements.

[48] *See* Exhibit B (compendium of Apple's *App Review Guidelines* from 2018 to 2025). *See also* Apple Developer, *App Review Guidelines*, available at https://developer.apple.com/app-store/review/guidelines/ (last visited Aug. 27, 2025).

[49] *See* Apple Developer, *App Review*, https://developer.apple.com/distribute/app-review/ (last visited Aug. 27, 2025).

D. Apple's Long-Term Campaign Cultivated and Secured Consumer Reliance

67. Apple has successfully cultivated the impression that its products and the apps it vets and makes available in the App Store are safe and trustworthy. The typical user of Apple's devices is not a cybersecurity expert, and therefore "must rely upon information gathered through interactions with [the App Store] to make decisions about the security implications of the apps they download."[50, 51] Consumers therefore "must depend on the app stores to protect them from malicious software and to clearly communicate possible risk."[52]

68. Research confirms that "most consumers trust the official markets associated with their platform to deliver safe applications,"[53] discounting potential concerns about the apps they download from the App Store "in favor of a reliance on trust in these institutions."[54] Consumers "are willing to trust apps they download from app stores because of years of positive experiences with the extra scrutiny and safeguards app stores offer. Simply being available on the app stores is now an indicator that an app is reasonably trustworthy for consumers."[55] Research into mobile

---

[50] David Schuster et al. (2015), *Opinions or Algorithms: An Investigation of Trust in People Versus Automation in App Store Security*. Found in: Theo Tryfonas et al., *Human Aspects of Information Security, Privacy, and Trust*, Lecture Notes in Computer Science, vol. 9190 (2015), available at https://doi.org/10.1007/978-3-319-20376-6_37 (last visited Aug. 21, 2025).

[51] *See also* Alexios Mylonas et al., *Delegate the smartphone user? Security awareness in smartphone platforms*, 34 Computers & Security 47–66 (2013), available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404812001733?via%3Dihub (last visited Aug. 21, 2025) (discussing research finding that users who are not technology or security savvy are more like to trust official app repositories like the App Store).

[52] David Schuster et al., *supra* footnote 50 at 415.

[53] Mark A. Harris et al., *Mobile App Installation: the Role of Precautions and Desensitization*, 24 Journal of International Technology and Information Management 47, 49 (2015), available at https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1052&context=jitim (last visited Aug. 21, 2025); *see also* Mylonas et al., *supra* footnote 51 at 60 ("The findings of the survey analysis show that the majority of smartphone users believe that downloading applications from the app repository is risk-free.").

[54] Amita Goyal Chin et al., *A bidirectional perspective of trust and risk in determining factors that influence mobile app installation*, 39 Int'l J. of Info. Mgmt. 49, 51 (2018), available at https://www.sciencedirect.com/science/article/abs/pii/S0268401217304309?via%3Dihub.

[55] The App Association, *Security and Trust from an App Maker's Point of View*, ACT online (Nov. 2021), available at https://actonline.org/wp-content/uploads/App-Association-Security-and-Trust-from-an-App-Makers-Point-of-View-November-2021.pdf (last visited Aug. 21, 2025); *see*

commerce (including app downloads) found participants "repeatedly purchased from the same places and this history made them feel safer and lead[s] to them trusting the company and their activities with it."[56]

69. Consumers also trust apps from the App Store because they trust Apple itself. This is part of a successful branding strategy and the goal of branding strategies, generally. And this is the precise outcome Apple's branding strategy seeks: consumers transfer their trust in Apple as a company to every app it approves and offers in the App Store. One study into mobile commerce found consumers trust apps because Apple—a trusted company—vets and approves all the apps in the App Store:

> [Research] participants mentally transferred their trust from larger companies (e.g., Apple) that approved mCommerce [mobile commerce] applications to the applications themselves.... For example, if participants were using an app on their mobile device ... because the app had been approved through a larger trusted company (e.g., Apple), the trust the participant had with that company transferred to the app itself. A similar phenomenon occurred for purchasing or downloading apps themselves. Because apps were approved by a larger, trusted company, apps themselves were considered to be trustworthy.
>
> For example, many participants said that apps found in the Apple store were trustworthy because, as consumers, they felt they were protected by the Apple brand and the 'prescreening' that the company does before permitting an app to be present in the store.

Participants explained, for example, that "everything is prescreened in the (Apple) app store, so there is no worry about (trust)," and that without Apple's protections "it just feels like you are opening up your phone to all the internet and random companies."[57] In short, consumers equate Apple's endorsement with safety.

---

also Mylonas et al., *supra* footnote 51 at 60 ("First, the fact that an app is distributed from an official app repository may mislead the users into believing that the app is secure ....").

[56] Serena Hillman, et al., *Soft Trust and mCommerce Shopping Behaviors*, *in MobileHCI '12: Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services* 113, 118 (Ass'n for Computing Mach. 2012), available at https://clab.iat.sfu.ca/pubs/SoftTrustMobileHCI.pdf (last visited Aug. 21, 2025).

[57] *Id.* at 118–19 (italics in original); *see also id.* at 118 ("*'[the] Apple App store is an official app for Apple brand and since Apple is a famous brand so I have no problem trusting and purchasing online with them.' – P8*." (alteration and italics in original)).

70. As one study concluded, for App Store users, "the (often stringent) approval processes (e.g., Apple's App Store) that mobile apps must go through before they are even placed in the hands of consumers acts as a guarantor of service or products acquired through it."[58]

E. Apple's Knowledge of Fraud and Concealment of Red Flags

71. Apple knew or should have known that this consumer reliance was occurring against the backdrop of growing fraud warnings. Rather than strengthen protections in light of this knowledge, Apple prioritized preserving the trust narrative that it had cultivated for decades.

72. Apple and other sophisticated digital actors are well aware of the threat of these schemes. Apple knew (or should have known) that these types of frauds exist. Instead of protecting consumers, they assist the cyberthieves and, specifically, pig-butchering scams, by telling Plaintiffs and Class members that these apps have been vetted and can be trusted. Despite representations that Apple takes App Store security seriously, that its customers can trust what is available in the App Store, and that App Store apps used to trade cryptocurrency meet all relevant legal requirements, Apple allowed these fraudsters to place their apps for download in the App Store and caused great harm to Plaintiffs and Class members.

73. Apple maintains exclusive knowledge of material facts regarding the fraudulent apps not known to Plaintiffs and Class members i.e., that it has not adequately vetted the apps and the cybercriminals behind the apps and that the apps are not safe, should not be trusted, and are being used for pig butchering frauds. Yet Apple actively concealed or suppressed those material facts from Plaintiffs and Class members. As such, Apple had a duty to disclose to Plaintiffs and Class members that the apps were not safe and should not be trusted, and Apple failed to implement and maintain reasonable security procedures and practices to properly vet, review, monitor and remove the fraudulent apps from its App Store.

74. Apple was on notice long before Plaintiffs' losses. Security researchers and media reports documented "pig-butchering" scams infiltrating the App Store as early as 2021. Apple also received consumer complaints about the very apps at issue, including Digicoins and SolLuna, prior

[58] *Id.* at 121.

to Plaintiffs' downloads. Apple requires developers to submit licensing information for financial apps, yet these apps lacked such credentials. By allowing unlicensed, fraudulent financial apps to remain in the App Store, Apple ignored red flags that were apparent through its own vetting process.

75. Despite this knowledge and its promises, Apple failed to take adequate and reasonable measures to ensure that the fraudulent apps are not available for download from the App Store, or to remove them once consumers complained about the fraud, and to date continues to permit such fraudulent apps to be downloaded from the App Store, which leads to the damage and harm described herein.

76. Apple's refusal to remove the apps or notify users was not mere negligence but a deliberate choice to protect its image and revenues. Apple's concealment of material facts—that these apps were unsafe, unlicensed, and fraudulent—directly caused Plaintiffs' losses.

F. Fraudsters Exploit Apple's Long-Term Campaign and Assistance

77. Consistent with Apple's long-term advertising campaign goal of fostering trust in App Store apps, by virtue of being Apple approved and available in Apple's App Store, Apple users trusted the fraudulent pig-butchering apps at issue, which themselves exploit trust. In reporting on pig butchering scams in the App Store, one article in 2023 observed that the "presence of the apps in the App Store made the ruse all the more convincing."[59]

78. Similarly, researchers at the cybersecurity firm SophosLabs warned about pig butchering apps being available in the App Store, stressing that "[i]f criminals can get past these checks [Apple purports to conduct], they have the potential to reach millions of devices. This is what makes it more dangerous for [scam app] victims, as most of those targets are more likely to trust the source if it comes from the official Apple App Store."[60]

---

[59] Dan Goodman, *Pig-butchering scam apps sneak into Apple's App Store and Google Play*, Ars Technica (Feb. 1, 2023), available at https://arstechnica.com/information-technology/2023/02/pig-butchering-scam-apps-sneak-into-apples-app-store-and-google-play/ (last visited Aug. 21, 2025).

[60] Jagadeesh Chandraiah, *Fraudulent 'CryptoRom' trading apps sneak into Apple and Google app store*, Sophos News (Feb. 1, 2023), available at https://news.sophos.com/en-us/2023/02/01/fraudulent-cryptorom-trading-apps-sneak-into-apple-and-google-app-stores/ (last visited Aug. 21, 2025).

79. Rather than the traditional separation of hardware and software, Apple has acknowledged that its entire business model is based on the interconnection between both elements, with Apple's range of devices supported by digital content and apps offered through the App Store.[61] Analysts credit Apple's "centralized and integrated digital ecosystem that seamlessly links products with the electronic marketplace" as a key driver of Apple's large market share.[62] Apple admits that "[s]urvey data has shown that consumers have ranked 'malware protection' and 'privacy' as the most important features in Apple's App Store."[63] Thus, Apple's business model and hardware sales depend on the impression Apple has purposely created that App Store applications are safe and secure for Apple customers.

80. Apple maintains rigorous control over which applications can be installed on its devices, permitting downloads only through the App Store. Other than through this so-called "walled garden," Apple customers have no practical or convenient way to obtain apps for their iPhones or iPads. As alleged above, Apple's restriction of available apps to only those published in the App Store reinforces its message that its platform is safer than competitors.[64] If App Store applications are not perceived to be safe, the sales of iPhones and iPads will be directly and negatively impacted.

81. Apple also benefits from App Store downloads even when it does not take a direct cut of revenue. By drawing consumers into its exclusive marketplace, Apple reinforces the appeal of its ecosystem, which in turn drives sales of its profitable hardware devices and discourages consumers from purchasing competing products. "[A] key facet of the Apple business model is ensuring that Apple content can only be played on Apple devices, as this helps maintain digital

---

[61] Birgitta Bergvall-Kåreborn & Debra Howcroft, *The Apple business model: Crowdsourcing mobile applications*, 37 Accounting Forum 280, 282 (2013), available at https://www.tandfonline.com/doi/full/10.1016/j.accfor.2013.06.001 (last visited Aug. 21, 2025).

[62] *Id.*

[63] *See In re Apple iPhone Antitrust Litigation*, No. 4:11-cv-06714 (N.D. Cal.), ECF No. 1004-1 (Supporting Separate Statement of Undisputed Material Facts), at 9.

[64] *See* Harris et al., *supra* footnote 53 at 49.

download market share and in turn drives sales volume for profitable hardware devices."[65] While Apple hardware is available through many retailers, digital content for Apple devices is available only through the App Store.[66] Apple's own annual reports confirm this strategy, noting Apple's belief that "decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services" and so Apple "relies on the continued availability and development of compelling and innovative software applications for its products."[67]

82. The App Store's perception of trust and safety has "been central to the growth in app downloads and usage over time."[68] Thus, as alleged here, Apple intentionally cultivates an impression of trustworthiness amongst consumers, including that apps on the App Store are highly vetted and safe for users to download and use.[69] One consumer research analyst explained that consumer trust in Apple leads to consumer use and spending with Apple: "The more consumers trust a brand, the more they use that brand.... Apple's huge installed base of trusting users has tremendous value, driving a high level of spend with the brand."[70]

83. Because Plaintiffs knew from Apple's repeated representations and long-term advertising campaign that all App Store applications were thoroughly reviewed, vetted, and safe, they reasonably relied on those assurances when purchasing Apple hardware (i.e., iPhones and iPads) and when downloading one or more of the fraudulent cryptocurrency trading applications.

---

[65] Johnna Montgomerie & Samuel Roscoe, *Owning the consumer—Getting to the core of the Apple business model*, 37 Accounting Forum 290, 291 (2013), available at https://www.sciencedirect.com/science/article/pii/S015599821300032X.

[66] *See id.*; *see also* Bergvall-Kåreborn & Howcroft, *supra* footnote 61 at 282.

[67] Apple, *Form 10-k*, Apple (2024), available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0000320193/c87043b9-5d89-4717-9f49-c4f9663d0061.pdf (last visited Aug. 21, 2025).

[68] Juliette Caminade & Jonathan Borck, *The Continued Growth and Resilience of Apple's App Store Ecosystem*, Apple (May, 2023), available at https://www.apple.com/newsroom/pdfs/the-continued-growth-and-resilience-of-apples-app-store-ecosystem.pdf.

[69] *Id.* at 20 ("Apple has heavily invested in the development of policies to foster user trust and the deployment of resources to enforce them.").

[70] David Myhrer, *How Brand Trust and a Strong Product Portfolio Drives Apple's Success*, IDC (Feb. 12, 201), available at https://blogs.idc.com/2021/02/12/how-brand-trust-and-a-strong-product-portfolio-drives-apples-success/ (last visited Aug. 21, 2025).

84. The fraudsters that carried out the pig butchering schemes against Plaintiffs and Class members through the App Store did so specifically because the apps being in the App Store lent credibility to the scheme. They knew Apple advertises that App Store as being a safe and trustworthy platform, and they exploited those representations to carry out the fraud.

G. Digital Asset Frauds: How the Scheme Operates

85. With Apple's trust and safety message in mind, Plaintiffs downloaded apps reasonably trusting that the apps would be safe to use, legitimate, and suitable for conducting secure financial transactions. Instead, Plaintiffs were met with digital asset fraud, finding themselves victims of schemes that Apple's promises of safety should have prevented.

86. Fraudsters can carry out these digital asset frauds in different ways. One common mechanism is to "claim to invest customers' funds in proprietary crypto trading systems or in 'mining' farms. The fraudsters promise high guaranteed returns (for example, 20-50%) with little or no risk."[71]

87. Fraudsters can create fake "trading" platforms in which they convince people to deposit money in what they believed was their own account under their control to purchase an investment. They often starting with small purchases, then are shown that those investments are paying off, thereby encourage the consumer to deposit more money for the purpose of purchasing ever-larger investments. The fraudster continues promising the users that they are trading their money and achieving high returns.[72] In reality, no investment is purchased and "no trading actually takes place."[73] Any money deposited into the platform is stolen by the scammers. "When victims

[71] Commodity Futures Trading Commission, *Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites*, CFTC.gov, available at https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html#:~:text=Be%20wary%20of%20anyone%20who,that%20is%20difficult%20to%20understand. (last visited Aug. 21, 2025).

[72] Commodity Futures Trading Commission, *Digital Asset Frauds*, CFTC.gov, available at https://www.cftc.gov/LearnAndProtect/digitalassetfrauds (last visited Aug. 21, 2025).

[73] *Id.*

try to withdraw their earnings, suddenly there is a problem, or they are told they must pay out-of-pocket to cover exorbitant undisclosed fees or fake taxes."[74]

88. These cryptocurrency scams are extremely prevalent. The FBI recently reported that the total amount of money lost in these frauds in 2023 was over $5.6 billion.[75] Investment scams, such as the ones discussed above and at issue here, "accounted for 71% of all crypto-related losses" in 2023.[76] The U.S. Secret Service has warned that these types of frauds are of "national interest."[77]

89. Apple was well aware, or should have been aware, of the prevalence of these scams and the specific risks they posed to its customers. Despite red flags from security researchers, media reports, and direct consumer complaints—including from Apple's own customers who reported the fraudulent apps—Apple failed to take meaningful corrective action. Instead, it continued to represent its App Store as safe and trustworthy, knowing consumers would rely on those assurances. As a result, Plaintiffs and Class members placed their confidence in Apple, downloaded fraudulent apps from the App Store, and suffered devastating financial losses.

PLAINTIFFS' EXPERIENCES

A. Plaintiff Sandeep Kapil's Experience

90. In August 2023, Plaintiff Kapil joined an online investment discussion group whose purported objective was to share stock recommendations, investment strategies and to leverage the combined investment resources of the group. At the behest of the group leader, an individual using the name Kevin Wilson, a claimed financial expert who professed to have multiple degrees and a prestigious employment history, the Wilson discussion group expanded into trading cryptocurrency.

---

74 *Id.*

75 Hannah Lang, *Losses from Crypto Scams Grew 45% in 2023, FBI Says*, Reuters (Sept. 9, 2024), available at https://www.reuters.com/technology/losses-crypto-scams-grew-45-2023-fbi-says-2024-09-09/ (last visited Aug. 21, 2025).

76 *Id.*

77 United States Secret Service, *Combating the Illicit Use of Digital Assets*, SecretService.gov, available at https://www.secretservice.gov/investigations/digitalassets (last visited Aug. 21, 2025).

91. Kapil and other group members were encouraged to join the supposed cryptocurrency trading platform called Digicoins and utilize the $200 to $800 provided by the exchange to start trading. Kapil was told to download the Digicoins app from the Apple App Store.

92. Kapil has been an avid user of Apple products for more than two decades. Between 2014 and present day, Kapil has purchased eight iPhones for himself and his family directly from Apple. He believed Apple was a trustworthy company that provided safe, secure, and trustworthy products and services, including apps from the App Store. He trusted apps from the App Store because of his general belief about Apple, confirmed by his experience with Apple products and his experience downloading and using other apps on the App Store, including apps that he used only because he believed App Store apps were secure such as an app for on-line banking. Kapil also trusted the Digicoins app because of the long-term advertising campaign message Apple has conveyed to the public and its customers—that apps on the App Store are vetted, safe, and trustworthy. Kapil's confidence arose from Apple's long-term advertising campaign marketing the App Store as a secure platform, where all apps meet rigorous safety standards.

93. Kapil generally reads or watches both traditional and non-traditional media and is exposed to marketing and publicity material in a variety of forms. Kapil saw and was exposed to Apple's long-term advertising campaign regarding the App Store and its apps in a variety of forms, including the media, television advertising, product release advertising, internet advertising and website statements.

94. Specifically, Kapil relied on his understanding of Apple and the App Store and because he viewed and relied upon the following representations regarding the security of Apple and its App store:

(1) Kapil was exposed to Apple's television advertising and viewed numerous ad campaigns from 2008 to present which touted the App Store as a secure, vetted place for downloading iPhone apps. Through that exposure, Kapil viewed, *inter alia,* the ad campaign "There's an app for that" series, which Apple launched in 2008 and which Kapil viewed in or around 2008. Exposure to such advertising

led to Kapil's confidence that apps from the App Store were safe, vetted, and trustworthy.

(2) Beginning in 2020 and continuing periodically to the present, Kapil was exposed to and viewed the App Store website representations alleged above. Exposure to the App Store website representations further led to Kapil's confidence that apps from the App Store were safe, vetted and trustworthy.

(3) Kapil also read Apple's *App Review Guidelines* available on the App Store, including specific guidelines for cryptocurrency trading apps. Kapil read these guidelines in October 2023, shortly before depositing his first significant sum of money into the Digicoins app. Kapil was exposed to and relied on Apple's representations in the *App Review Guidelines*, including: "We do this by offering a highly curated App Store where every app is reviewed by experts…" and "Apps facilitating Initial Coin Offerings ("ICOs"), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law."[78] The *App Review Guidelines*, both generally and specific to digital trading apps, further led to Kapil's confidence that apps from the App Store were safe, vetted and trustworthy.

95. In reliance on this impression Apple has cultivated over time regarding the safety and security of App Store apps and based on his belief that the Digicoins app downloaded from Apple's App Store was safe and secure based on Apple's representations that the app had been reviewed by experts, adhered to Apple's guidelines for financial apps and was a legitimate cryptocurrency trading app as it purported to be, Kapil downloaded Digicoins from the App Store in or around the month of August, 2023, and began transferring money and buying cryptocurrency

[78] *See* Exhibit B (compendium of Apple's *App Review Guidelines*, including from 2023). *See also* Apple Developer, *App Review Guidelines*, available at https://developer.apple.com/app-store/review/guidelines/.

he believed he could use to conduct legitimate digital trades on the Digicoins app. Kapil downloaded the Digicoins app onto his iPhone XR that he purchased from Apple near the end of 2018 for approximately $1,000. Kapil would not have purchased his iPhone or spent as much money on the iPhone if he had known the truth about Apple's representations that its apps were not safe or trustworthy. He would not have downloaded the Digicoins app if had known it had not been properly vetted by Apple experts, did not meet guidelines for such apps and was not a safe, trustworthy and legitimate cryptocurrency trading app as represented by Apple.

96. Kapil's initial deposits were in relatively small amounts. Before he began transferring larger amounts to Digicoins he looked for additional assurance from Apple regarding the legitimacy and safety of the Digicoins app. To this end, Kapil reviewed Apple's guidelines and review process for apps available from the App Store, including the particular standards Apple purportedly requires for cryptocurrency exchange apps as alleged above. Apple's representations regarding the safety and security of apps on its App Store further convinced Kapil the Digicoins app was safe for his investments. In reliance on Apple's safety message, Kapil began to deposit in larger amounts and to participate—so he believed—in legitimate Initial Coin Offerings (ICOs). Kapil's reliance on Apple's representations was reasonable because the representations he relied on concern the safety and security of apps from the App Store—the "guiding principle" of the App Store according to Apple—and Kapil relied upon Apple's representations for these purposes.

97. By the end of January 2024, Kapil's Digicoins account had apparently increased from his investment amount of approximately $1,236,935 to over $1,465,991. But then, in early February 2024, Kapil's Digicoins account was suddenly locked and his assets in his account frozen. A few days later, the Digicoins app was non-functional and non-responsive. Kapil later discovered the Digicoin app was not legitimate or in compliance with legal requirements, contrary to Apple's representations, it was not safe and could not nor ever could be trusted, and it did not comport with Apple's represented standards and vetting processes for a cryptocurrency app. The Digicoins app was part of a "pig-butchering" scam and the more than $1,236,000 that Kapil had deposited was gone. As a direct result of Apple's process for reviewing the Digicoins app on its App Store and Kapil's reasonable reliance on Apple's representations assuring him the app had been vetted, was

safe and could be trusted, Plaintiff Kapil was injured and lost over a million dollars. Contrary to Apple's representations and stated processes for correction, Kapil and other users of Digicoins were never notified by Apple that Digicoins was a dangerous app used for fraud and malicious activity. Because of the false and deceptive material misrepresentations at issue, Plaintiff Kapil also overpaid for his iPhone.

B. Plaintiff Gabriela Gomez's Experience

98. On approximately August 2023, Plaintiff Gomez joined two online investment discussion groups whose purported objectives were to share stock recommendations, investment strategies and to leverage the combined investment resources of the group. Gomez had been educating herself by various means regarding stock investments and trading of digital assets and the online discussion groups were part of this process. At the behest of one of the group leaders, an individual using the name Kevin Wilson, who was a claimed financial expert with multiple degrees and a pedigreed employment history, Gomez expanded from stock trading to also attempting to trade in cryptocurrency.

99. Gomez and other Wilson discussion group members were encouraged to join the platform called Digicoins and utilize the $200 to $800 provided by the exchange to start "trading." The leader of Gomez's other investment group, Wade Brittingham, encouraged Gomez and other group members to join the platform SolLuna available for download on the Apple App Store.

100. Gomez has used Apple products for decades, since at least 2007. She believed Apple was a trustworthy company that provided safe, secure, and trustworthy products and services, including apps from the App Store. She trusted apps from the App Store because of her general belief about Apple, confirmed by her experience with Apple products, her experience with downloading and using other apps from the App Store, and because of the message Apple has conveyed to the public and its customers—that apps on the App Store are vetted, safe, and trustworthy. This confidence arose from Apple's long-term advertising campaign marketing the App Store as a secure platform, where all apps meet rigorous safety standards.

101. Gomez generally reads or watches both traditional and non-traditional media and is exposed to marketing and publicity material in a variety of forms. Gomez was exposed to Apple's

long-term advertising campaign regarding the App Store and its apps in a variety of forms, including Apple's television advertising, in-store advertising, product release advertising and internet advertising.

102. Specifically, Gomez viewed and relied upon the following representations regarding the security of Apple and its App Store:

(1) Gomez was exposed to Apple's television advertising and viewed numerous ad campaigns from 2008 to present which presented the App Store as a secure, vetted place for downloading iPhone apps. Gomez recalls the "There's an app for that" advertising series, which launched in 2008 and which Gomez viewed in or around 2009. Exposure to this advertising campaign led to Gomez's confidence and belief that apps from the App Store safe, vetted and trustworthy.

(2) Gomez was also exposed to Apple's advertising regarding the security and safety of App Store apps during her many visits to Apple retail stores, beginning in about 2012 to the present. Gomez recalls Apple employees in the Apple Store making representations about the App Store's safety and vetting process during her in-store visits. Exposure to employee statements further led to Gomez's confidence and belief that apps from the App Store were safe, vetted and trustworthy.

(3) Beginning in 2020 and continuing periodically through present day, Gomez was exposed to and viewed the App Store website representations alleged above. Exposure to the App Store website representations further led to Gomez's confidence that apps from the App Store were safe, vetted and trustworthy.

103. In reliance on this impression Apple has cultivated over time that apps on the App Store are vetted, safe, and trustworthy, including Apple's representations regarding the safety and security of App Store apps and based on her belief that the Digicoins and SolLuna apps downloaded from Defendant's App Store were safe and secure, Gomez downloaded Digicoins and SolLuna from the App Store and began transferring money and buying cryptocurrency she believed she could use to conduct legitimate digital trades on the apps. Gomez's reliance on Apple's representations was

reasonable because the representations she relied on concern the safety and security of apps from the App Store—the "guiding principle" of the App Store according to Apple—and Gomez relied upon Apple's representations for these purposes. Gomez used the App Store to download the Digicoins and SolLuna apps in or around the month of October 2023. Gomez downloaded the Digicoins and SolLuna apps onto her iPhone 11, model number NWKM2LL/A, that she purchased from Sprint[79] on or about January 30, 2023. Gomez would not have purchased her iPhone if she had known the truth about Apple's representations that its apps were not safe or trustworthy.

104. At the end of November 2023, Gomez attempted to withdraw some of her funds from SolLuna and was told she could not withdraw funds until she paid $10,000 in taxes she owed on the increased value of her money. Questioning the legitimacy of the request and the application as a whole, Gomez contacted Apple via Apple chat on November 30, 2023 and subsequently also spoke with an Apple representative. Apple assured Gomez that apps from the App Store were all tested and vetted for legitimacy and authenticity, and that she could safely continue to use the SolLuna app.

105. After speaking with Apple and receiving Apple's reassurance that SolLuna was vetted and safe, Gomez paid the $10,000 into her SolLuna app and continued to attempt to withdraw her funds. However, in mid-December when Gomez tried to withdraw funds from her SolLuna account, her request was refused unless she agreed to pay yet more money into the app for sums she purportedly owed the U.S. government. Convinced SolLuna was a scam, Gomez once again contacted Apple. Apple removed the SolLuna app a few days later. However, contrary to Apple's representations and stated processes for correction, Gomez and other users of SolLuna were never notified by Apple that SolLuna was a dangerous app used for fraud and malicious activity.

[79] Apple sells iPhones in large volumes to major carriers—including Sprint, Verizon, and AT&T—at wholesale prices. These carriers then resell the devices to consumers, but Apple collects full payment of the wholesale price from carriers upon delivery. *See* Andrew Orr, *Apple Inches up Share of Direct iPhone Sales but Carriers Dominate the Field*, Apple Insider (May 14, 2025), available at https://appleinsider.com/articles/25/05/14/apple-inches-up-share-of-direct-iphone-sales-but-carriers-dominate-the-field (last visited Aug. 22, 2025).

106. At the same time, Gomez began to suspect Digicoins might also be a scam. She tried to withdraw her funds from Digicoins in mid-December 2023 and was unable to do so. Gomez informed Apple that Digicoins was also a scam. However, Apple ignored the warnings and complaints and continued to make Digicoins available on the App Store for users to download and use under the false impression that Digicoins had been vetted, was safe, and could be trusted. It was not until February 2024 that Apple removed Digicoins from the App Store, and contrary to Apple's representations and stated processes for correction, Gomez and other users of Digicoins were never notified by Apple that Digicoins was a dangerous app used for fraud and malicious activity. In total, Gomez "invested" approximately $72,000 between the Digicoins and SolLuna apps. As a direct result of Apple's process for reviewing the Digicoins app on its App Store and Gomez's reasonable reliance on Apple's representations assuring her the apps had been vetted, was safe and could be trusted, Plaintiff Gomez was injured and lost approximately $72,000. Because of the false and deceptive material misrepresentations at issue, Plaintiff Gomez also overpaid for her iPhone.

C. Plaintiff Kim Sallen's Experience

107. In the fall of 2023, Plaintiff Sallen joined an online investment discussion group whose purported objective was to share stock recommendations, investment strategies and to leverage the combined investment resources of the group. Sallen had been educating herself by various means regarding stock investments and trading of digital assets and the online discussion group was part of this process. At the behest of the group leader, an individual using the name Kevin Wilson, who was a claimed financial expert with multiple degrees and a pedigreed employment history, Sallen was encouraged to join the platform called Digicoins, available for download on the Apple App Store, and utilize the $200 to $800 provided by the exchange to start "trading." Sallen downloaded the Digicoins app from the App Store in or around September 2023. In September or October 2023, Sallen was directly contacted by an individual she believed was a member of the Kevin Wilson investment discussion group. This man was purportedly an expert in real estate contracts and contracts trading, including cryptocurrency. He offered to work with Sallen regarding trading of cryptocurrency contracts and commodities contracts. He used Forex5 as a trading

platform for such trades and suggested Sallen download the Forex5 app, which was available on the Apple App Store. Sallen downloaded Forex5 from the App Store in or around October 2023.

108. Sallen has used Apple products for approximately 20 years. She believed Apple was a trustworthy company that provided safe, secure, and trustworthy products and services, including apps from the App Store. She trusted apps from the App Store because of her general belief about Apple, confirmed by her experience with Apple products, her experience with downloading and using other apps from the App Store, and the overall impression Apple has cultivated among its customers—that apps on the App Store are vetted, safe, and trustworthy. This confidence arose from Apple's long-term marketing campaign that the App Store is a secure platform, where all apps meet rigorous safety standards.

109. Sallen generally reads or watches both traditional and non-traditional media and is exposed to marketing and publicity material in a variety of forms. Sallen was exposed to Apple's long-term advertising campaign regarding the App Store and its apps in a variety of forms, including Apple's television advertising, product release advertising and internet advertising.

110. Specifically, Sallen viewed and relied upon the following representations regarding the security of Apple and its App store:

(1) Sallen was exposed to Apple's television advertising and viewed numerous ad campaigns which touted the App Store as a secure, vetted place for downloading iPhone apps. Through that exposure, Sallen viewed, *inter alia*, the ad campaign "If it's not an iPhone" series, which launched in 2015 and which Sallen viewed in or around that time. Exposure to such advertising led to Sallen's confidence and belief that apps from the App Store were safe, vetted, and trustworthy.

(2) Sallen's confidence in the App Store's safety was reinforced by her knowledge that her large corporate employer, as well as other major corporations, issued iPhones to their employees for business use. From March 2016 through August 2021, Sallen owned and used Apple iPhones provided through her employer, including App Store apps downloaded to her iPhone, receiving a new device approximately every two years. To her, this confirmed that Apple devices and

App Store apps were trusted as secure not only by individual consumers, but by sophisticated enterprises. Sallen's iPhones provided by her employer were in addition to the iPhones she purchased for her personal use, including the iPhone on which she downloaded the fraudulent apps.

(3) Beginning in 2020 and continuing periodically through present day, Sallen was exposed to and viewed the App Store website representations alleged above. Exposure to the App Store website representations further led to Sallen's confidence that apps from the App Store were safe, vetted and trustworthy.

(4) In September 2023, before she downloaded a cryptocurrency trading application from the App Store, Sallen visited and read the *App Review Guidelines*, including the specific section for cryptocurrency trading apps. There, Sallen was exposed to and relied on Apple's representations, including that "Apps facilitating Initial Coin Offerings ("ICOs"), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law."[80] The *App Review Guidelines* specific to digital trading apps further led to Sallen's confidence and belief that apps from the App Store were safe, vetted and trustworthy.

111. In reliance on this impression Apple has cultivated over time that apps on the App Store are vetted, safe, and trustworthy, including Apple's representations regarding the safety and security of App Store apps and based on her belief that the Digicoins and Forex5 apps downloaded from Defendant's App Store were safe and secure, Sallen downloaded Digicoins and Forex5 from the App Store and began transferring money into what she believed were her accounts and buying and trading in cryptocurrency and other assets. Sallen's reliance on Apple's representations was

[80] *See* Exhibit B (compendium of Apple's *App Review Guidelines*, including from 2023). *See also* Apple Developer, *App Review Guidelines*, available at https://developer.apple.com/app-store/review/guidelines/.

reasonable because the representations she relied on concern the safety and security of apps from the App Store—the "guiding principle" of the App Store according to Apple—and Sallen relied upon Apple's representations for these purposes. Sallen downloaded the Digicoins and Forex5 apps onto her iPhone 12, model number MGF73LL-A, that she purchased on August 17, 2021 when she opened an account with Verizon. Sallen would not have purchased an iPhone if she had known the truth about Apple's representations that its apps were not safe or trustworthy.

112. In mid-December 2023, Sallen was contacted and informed she was required to pay over $79,000 into her Forex5 app. Sallen questioned Forex5 regarding the payment demand and the responses from Forex5 began to change as regards the reasons she was required to pay the above amount. Soon the app and its customer service stopped responding to Sallen's inquiries and she was locked out of the Forex5 app. Sallen could not withdraw her funds and she lost approximately $60,000 to the Forex5 scam. She reported the Forex5 app to Apple via "app review." Despite being on notice of the fraudulent app in its App Store, for months, Apple took no action to remove the app from its App Store. After several additional contacts and conversations between Sallen and Apple from late December 2023 to March 2024, Apple finally removed Forex5 from its App Store in or around March 2024. Apple never notified users of the Forex5 app that the app was dangerous and used for fraud.

113. In early January 2024, Sallen began to suspect that Digicoins was also a scam and attempted to pull her money out of what she thought was her Digicoins account. Sallen was at first told others were able to close out and therefore any difficulty must be at her end. In response to additional attempts and inquires, Sallen was told she would be able to withdraw her funds following routine maintenance of the application. Shortly thereafter, the app and customer support stopped responding and Sallen was shut out of the Digicoins app. Sallen lost approximately $60,000 to the Digicoins scam. And contrary to Apple's representations and stated processes for correction, Sallen and other users of Digicoins were never notified by Apple that Digicoins was a dangerous app used for fraud and malicious activity.

114. As a direct result of Apple's inadequate process for reviewing the Digicoins and Forex5 apps on its App Store and Sallen's reasonable reliance on Apple's representations assuring

her the apps had been vetted, were safe and could be trusted, Plaintiff Sallen was injured and lost approximately $120,000. Because of the false and deceptive material misrepresentations at issue, Plaintiff Sallen also overpaid for her iPhone.

D. Plaintiff Danyell Shin's Experience

115. On or about September, 2024, Shin joined an online investment discussion group whose purported objective was to share stock recommendations, investment strategies, and to leverage the combined investment resources of the group. Shin had been educating herself by various means regarding stock investments and trading of digital assets and the online discussion group was part of this process. At the behest of the group leader, an individual using the name Daniel Mills, who was a claimed financial expert with a pedigreed employment history, the Mills discussion group expanded into trading cryptocurrency. Shin and the other group members were encouraged to download and join an app called Swiftcrypt from either the App Store or the Google Play Store and utilize the $100 to $2,000 provided by the exchange to start "trading."

116. Shin has used Apple products for at least 15 years. Most of those products, including the iPhone 13 used to download Swiftcrypt, Shin purchased directly from Apple. She believed Apple was a trustworthy company that provided safe, secure, and trustworthy products and services, including apps from the App Store. She trusted apps from the App Store because of her general belief about Apple, confirmed by her experience with Apple products, her experience with downloading and using other apps from the App Store, and the overall impression Apple has cultivated among its customers—that apps on the App Store are vetted, safe, and trustworthy. This confidence arose from Apple's long-term advertising campaign message that the App Store is a secure platform, where all apps meet rigorous safety standards.

117. Shin generally reads or watches both traditional and non-traditional media and is exposed to marketing and publicity material in a variety of forms. Shin was exposed to Apple's long-term advertising campaign regarding the App Store and its apps in a variety of forms, including television advertising, product release advertising, and internet advertising.

118. Specifically, Shin viewed and relied upon the following representations regarding the security of Apple and its App store:

(1) Shin was exposed to Apple's television advertising and viewed numerous ad campaigns which touted the App Store as a secure, vetted place for downloading iPhone apps. Through that exposure, Shin viewed, *inter alia*, the ad campaign "If it's not an iPhone" series, which launched in 2015 and which Shin viewed in or around that time. Exposure to such advertising led to Shin's confidence and belief that apps from the App Store were safe, vetted, and trustworthy.

(2) In 2024, before downloading the Swiftcrypt app from the App Store, Shin was also exposed to and viewed the App Store website representations. Exposure to the App Store website representations further led to Shin's confidence that apps from the App Store were safe, vetted and trustworthy.

119. In reliance on this impression Apple has cultivated over time that apps on the App Store are vetted, safe, and trustworthy, including Apple's representations regarding the safety and security of App Store apps and based on her belief that the Swiftcrypt app downloaded from the App Store was safe and secure, Shin downloaded Swiftcrypt onto her iPhone 13 Pro Max in or about September, 2024.

120. Shin's reliance on Apple's representations was reasonable because the representations she relied on concern the safety and security of apps from the App Store—the "guiding principle" of the App Store according to Apple—and Shin relied upon Apple's representations for these purposes. Plaintiff Shin would not have purchased an iPhone or spent as much on her iPhone if she had known the truth about Apple's representations and that its apps were not safe or trustworthy.

121. After relying on Apple's representations about the safety and vetting of apps in the App Store and downloading the Swiftcrypt app, Shin began transferring money into what she believed was her account and buying and trading in cryptocurrency and Initial Coin Offerings (ICOs). Between September, 2024, and mid-January, 2025, Shin transferred approximately $80,000 into the Swiftcrypt app, including approximately $50,000 obtained through a loan from her

husband's 401(k) account. By mid-January, 2025, Shin's Swiftcrypt account appeared to have increased to $421,000.

122. On or about January 14, 2025, Shin's Swiftcrypt account was suddenly locked and her assets in her account frozen. A few days later, the Swiftcrypt app became non-functional and non-responsive. Shin later discovered the Swiftcrypt app was not legitimate or in compliance with legal requirements. Contrary to Apple's representations, it was not safe and could not be trusted, and it did not comport with Apple's represented standards and vetting processes for a cryptocurrency app. The Swiftcrypt app was part of a "pig-butchering" scam and the more than $80,000 that Shin had deposited was gone. As a direct result of Apple's process for reviewing the Swiftcrypt app on its App Store and Shin's reasonable reliance on Apple's representations assuring her the app had been vetted, was safe, and could be trusted, Shin was injured and lost approximately $80,000. Contrary to Apple's representations and stated processes for correction, Shin and other users of Swiftcrypt were never notified by Apple that Swiftcrypt was a dangerous app used for fraud and malicious activity. Because of the false and deceptive material misrepresentations at issue, Shin also overpaid for her iPhone.

CLASS ACTION ALLEGATIONS

123. Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to the provisions of Federal Rules of Civil Procedure Rules 23(a), (b)(2), and (b)(3), on behalf of the class defined as:

> All persons who downloaded a cryptocurrency trading app from the Apple App Store within the relevant statutory period to the date notice is sent to the Class and whose funds were stolen from the cryptocurrency app by the app developers or agents working on their behalf.

124. Excluded from the Class are Defendant and its subsidiaries and related entities; all persons who make a timely election to be excluded from the Class; governmental entities; and any judge to whom this case is assigned and his/her immediate family. Plaintiffs reserve the right to revise the Class definition based upon information learned through discovery.

125. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claim.

126. This action has been brought and may be properly maintained on behalf of the Class proposed herein under Federal Rule of Civil Procedure 23 for the following reasons:

Numerosity

127. Pursuant to Federal Rule of Civil Procedure 23(a)(1), the members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are hundreds of members of the Class, the precise number of Class members is unknown to Plaintiffs but may be ascertained from Defendant's records. Class members may effectively and efficiently be notified of the pendency of this action by recognized, Court-approved dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or publication.

Commonality and Predominance

128. Pursuant to Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3), this action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct constituted violations of state consumer protection laws and negligent misrepresentation;

c. Whether Plaintiffs and the other Class members are entitled to damages, restitution or other monetary relief and, if so, in what amount; and

d. Whether injunctive relief is appropriate, including corrective advertising regarding the safety of App Store apps, and the form thereof.

Typicality

129. Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were injured through Defendant's wrongful conduct as described above.

Adequacy

130. Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs have retained experienced counsel competent in complex multi-party and class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

Superiority

131. Class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this action as a class action. The damages suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Apple, so it would be impracticable for members of the proposed Class to individually seek redress from the courts. Even if the individual Class members could afford to undertake individual litigation, such individual claims would unnecessarily burden the court system should they do so. Furthermore, individual litigation creates potential for inconsistent or contradictory orders and judgments and increases delay and expense to the parties and to the court system. A class action would present fewer administrative difficulties, would be more efficient, and would enhance the interests of consistent and fair justice in this matter.

132. In the alternative, the Class also may be certified because Defendant has acted or refused to act on grounds generally applicable to the Class thereby making final declaratory and/or injunctive relief with respect to the members of the Class as a whole, appropriate.

133. Plaintiffs seek preliminary and permanent injunctive and equitable relief on behalf of the Class, on grounds generally applicable to the Class, to enjoin and prevent Defendant from engaging in the acts described, and to require Defendant to provide relief to Plaintiffs and Class members.

134. Unless the Class is certified, Defendant will retain monies that were taken from Plaintiffs and Class members as a result of Defendant's wrongful conduct. Unless a classwide

injunction is issued, Defendant will continue to commit the violations alleged and the members of the Class and the general public will continue to be misled.

COUNT I

Violations of the Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*

135. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

136. Plaintiffs and Defendant are "persons" within the meaning of the UCL. Cal. Bus. & Prof. Code § 17201.

137. The UCL defines unfair competition to include any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. Prof. Code § 17200.

138. As a result of engaging in the conduct alleged in this Complaint, Defendant has violated each prong of the UCL.

A. Violations of the UCL's proscription against "unfair" business acts or practices.

139. Defendant's conduct as alleged in the Complaint violates the UCL's prohibition of "unfair" business practices because Defendant's business practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. Because of Apple's unscrupulous and unethical conduct, consumers have lost substantial amounts of money using App Store apps that were not legitimate, vetted or safe as represented by Apple. There is no utility or legitimate business purpose for Apple's conduct in that Apple by its express representations and long-term campaign promises that apps from its App Store are legitimate, safe and secure and can be downloaded with confidence because of Apple's vetting process and security standards. However, because Apple has prioritized profit over ethics, Apple fails to adequately vet predatory, potentially devastating "pig-butchering" cryptocurrency scam apps and makes them available to download despite its continuing misrepresentations that the apps in its App Store are vetted, safe and trustworthy.

140. Apple's conduct also violates the UCL's "unfair" prong because Apple's business practices undermine public policies aimed at protecting consumers from harm, especially in digital marketplaces. California, in particular, has a strong public policy in favor of safeguarding consumers

against deceptive practices and ensuring that products and services available to the public do not pose undue risk of fraud or financial loss. California's public policy encourages protecting citizens from financial scams and fraudulent schemes, particularly in digital markets where consumers are more vulnerable. For example, California's Department of Financial Protection & Innovation (DFPI) functions inter alia "to regulate financial services and products in California" including cryptocurrency and trading in cryptocurrencies and since 2022 the role of the DFPI "in overseeing crytpo has grown" to achieve California's policy of "protect[ing] every Californian from scams …" www.dfpi.ca.gov/consumers/crypto. The DFPI collects and reviews consumer complaints regarding cryptocurrency scams "for enforcement purposes and to inform policymakers." *Id*. In fact, the DFPI has a specific policy of protecting consumers from pig butchering scams and seeks to achieve this policy goal by informing consumers about pig butchering scams and asking consumers to report pig-butchering scams to the DFPI so such scams can be monitored for enforcement and to inform California policymakers. www.dfpi.ca.gov/consumers/crypto/what-are-pig-butchering-scams. In 2023, California policymakers enacted the Digital Financial Assets Law (DFAL) which inter alia requires entities that trade, store or exchange cryptocurrencies to be licensed by the DFPI with the policy goal of "promot[ing] consumer and investor protection …" www.dfpi.ca.gov/regulated-industries/digital-finanicial-assets.

141. The federal government also has a public policy of protecting citizens from financial scams and fraudulent schemes, particularly in digital markets where consumers are more vulnerable. For example, the Federal Trade Commission actively monitors and pursues cryptocurrency related scams and seeks to protect citizens from such scams by producing educational content and hosting public workshops on deceptive crypto practices. The FBI has an Internet Crime Complaint Center (IC3) that collects and analyzes reports of crypto-related fraud and shares the information and intelligence collected by IC3 with law enforcement and regulatory agencies to further investigations. The FBI also formed a Virtual Assets Unit that specializes in investigating crypto crimes. The Commodity Futures Trading Commission (CFTC) through its Office of Customer Education and Outreach seeks to further the federal government's policy of protecting citizens from crypto scams by distributing education materials to help the public recognize pig-butchering scams and

encouraging victims to report these scams to IC3. The CFTC also has a whistleblower program that offers rewards and protection to whistleblowers of cryptocurrency fraud. By allowing fraudulent apps that facilitate "pig-butchering" scams, Apple's conduct violates these public policies aimed at preventing fraud and financial exploitation.

142. Public policies also generally uphold the importance of transparency and truthfulness in advertising, especially when companies make safety and security claims. Apple's representations of App Store safety create a misleading sense of security, and violate policies against false advertising, including California's public policy against false advertising as reflected in the False Advertising Law, Bus. & Prof. Code § 17500 and federal public policy against false advertising and unfair business practices as reflected in the Federal Trade Commission Act, 15 U.S.C. §§ 41-58. There is also a public policy interest in maintaining high standards of digital security and privacy for consumers. Particularly given its representations to the contrary, Apple's failure to vet the cryptocurrency trading apps contravenes public policies intended to ensure that digital services, especially those related to finance, do not expose users to unnecessary risk. Public policy supports the principle that companies with substantial market control have a duty to protect users from known risks, especially where users cannot avoid these risks themselves. Apple's exclusive control over iOS app distribution heightens its duty to protect consumers, and its failure to do so conflicts with public policies focused on consumer protection in monopolized digital markets.

143. Apple also has engaged in unfair business practices under the "balancing test." because the injury to Plaintiffs and the Class is not outweighed by any countervailing benefits to consumers or competition, and the injury could not reasonably be avoided by Plaintiffs and the Class members. Plaintiffs and Class members do not have the resources and information regarding the apps and app developers to determine the legitimacy and safety of the App Store apps. In contrast, Apple as a condition of permitting apps on the App Store, requires app developers to provide it information from which Apple experts can vet the apps and determine their legitimacy and safety. There were reasonable available alternatives to further Defendant's legitimate business interests other than the conduct described herein. There is no countervailing benefit to consumers or

competition resulting from Apple's unfair business practice of permitting unsafe and un-vetted or inadequately vetted cryptocurrency trading apps on the App Store.

144. Plaintiffs were each subjected to Apple's unfair business practices and lost money as a result. Plaintiffs seek to have restored to them and the Class all money which has been acquired by means of the unfair competition alleged.

B. Violations of the UCL's proscription against "fraudulent" business acts or practices.

145. As a result of engaging in the conduct alleged in this Complaint, Apple has also violated the UCL's prohibition against fraudulent business acts or practices by representing that apps from its App Store are legitimate, safe and secure and can be downloaded with confidence because of Apple's vetting process and security standards.

146. Defendant's conduct as set forth fully above was false, misleading and/or likely to deceive a reasonable consumer.

147. A reasonable consumer would be deceived or mislead by Apple's representations because the representations regarding the legitimacy, safety and security of App Store apps are material to consumers' decision to purchase Apple hardware devices (iPhones and iPads) and material to consumers' decision to download and use App Store apps for financial transactions and related purposes.

148. Plaintiffs and other Class members have in fact been deceived as a result of their reliance on Apple's material misrepresentations. Plaintiffs would not have downloaded and used the cryptocurrency trading apps if they had known the apps were not vetted, safe and legitimate as represented by Apple.

C. Violations of the UCL's proscription against "unlawful" business acts or practices.

149. As a result of engaging in the conduct alleged in this Complaint, Apple has violated the UCL's proscription against engaging in "unlawful" conduct by virtue of its violations of California's Consumers Legal Remedies Act, Civil Code § 1750, violation of Civil Code §§ 1572, 1573, 1709, 1711, 1770(a)(5), (7), (9) and the common law. Plaintiffs reserve the right to allege other violations of law which constitute unlawful business acts or practices under the UCL.

150. Plaintiffs have suffered injury in fact and lost money or property as a result of Apple's unfair, fraudulent and unlawful business acts and practices alleged herein. Because of the unfair business practices at issue, Plaintiffs and members of the Class have suffered an injury in fact and have lost money and property, including, but not limited to, the expected utility and performance of their Apple iPhones and iPads, the purchase price of their Apple devices, and/or the difference between the price Class members paid and the actual worth of the hardware product had Apple disclosed the true nature of the representations at issue. As a result of Apple's misconduct and representations, including its substantial assistance and participation in the pig-butchering frauds perpetrated through the Apple App Store apps, Plaintiffs also invested and lost thousands of dollars in scam apps they acquired through Apple's App Store.

151. Apple's conduct in violation of the UCL is ongoing and continuing to this date. The unlawful, unfair and fraudulent business acts and practices of Defendant described herein present a continuing threat in that Apple is currently engaging in such acts and practices, and will persist and continue to do so unless and until an injunction is issued by this Court. Plaintiffs intend to continue to purchase App Store apps in the future if they are secure and comport with Apple's advertising claims and representations regarding its standards, vetting and review. Because Plaintiffs own Apple iPhones or iPads, and the ability to download and use apps is integral to the core functionality of the Apple devices they own, they have no reasonable, comparable alternatives except to download and use apps from Apple's App Store. If Apple is not enjoined from continuing its unfair business practices in violation of the UCL, Plaintiffs will not know whether the App Store apps, and especially financial apps, are safe, vetted and legitimate as represented and cannot safely use or download such apps in the future without subjecting themselves to other financial scams perpetrated via unvetted, scam App Store apps. Injunctive relief, in the form of corrective advertising, is also necessary to dispel public misperception about the safety and trustworthiness of apps in Apple's App Store that has resulted from years of Apple's unlawful marketing efforts and to prevent current and future Apple product users from being misled.

152. Plaintiffs lack an adequate legal remedy. In any event, any legal remedy that does exist is not adequate because inter alia, it is not equally prompt, certain, and in other ways efficient

as the equitable remedies proposed, including because the claims giving rise to potential legal remedies give rise to one or more legal defenses unavailable under Plaintiffs' theory under the UCL or impose more stringent elements than the UCL such that Plaintiffs may demonstrate their right to equitable relief (restitution or injunctive relief) under the UCL but fall short of establishing their right to legal damages under other claims or causes of action. Further, the scope of actionable misconduct under the unfair prong of the UCL is broader than the other available causes of action. Thus, Plaintiffs may ultimately be entitled to restitution or injunctive relief under the UCL, while not entitled to legal damages under other causes of action (e.g., the CLRA is limited to certain types of plaintiffs (an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes)).

153. Plaintiffs seek to have restored to them and the Class all money which has been acquired by means of the unfair competition alleged through scam cryptocurrency trading apps that Apple approved, promoted, and knowingly permitted to be offered and remain available on its App Store, and by overpaying for their Apple hardware devices, an injunction prohibiting Defendant from continuing the unfair business practices, corrective advertising, and all other relief this Court deems appropriate, consistent with Business & Professions Code § 17203.

COUNT II

Violations of Consumers Legal Remedies Act,
Cal. Civ. Code § 1750, *et seq.*

154. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

155. At all relevant times the Apple devices (e.g., iPhones or iPads), which include the App Store and applications available therein are goods or services that Apple has marketed and that Plaintiffs and Class members purchased or obtained for personal, family, or household purpose and, as such, are "goods" and "services" as defined by Cal. Civil Code sections 1761(a), (b).

156. Plaintiffs and Class members are individuals who purchased or leased and have used one or more Apple devices (e.g., iPhones or iPads) for personal, family or household purposes and,

as such, are "consumers" defined in Cal. Civil Code section 1761(d). Apple is a corporation and, as such, is a "person" as that term is defined in Cal. Civ. Code section 1761(c).

157. Plaintiffs and Class members purchased iPhones and iPads based at least in part on the mistaken belief and impression cultivated by Apple that the devices could be used to download safe and trustworthy apps vetted by Apple and available in the App Store, and that Apple does not permit apps that violate its developer guidelines (including requirements for safe and trustworthy cryptocurrency exchange apps). Plaintiffs and members of the Class would not have purchased the Apple hardware devices and/or would not have paid as much for them if Apple disclosed that the representations discussed herein were false and misleading.

158. In offering apps for download in the App Store onto Apple devices (e.g., iPhones or iPads), Apple represented expressly, by implication, and through a long-term advertising campaign that applications downloaded from the App Store are safe for use on the Apple devices. For example, Apple represents inter alia that "the App Store has proved to be a safe and trusted place to discover and download apps," that Apple is"[d]edicated to trust and safety," that "Apps must adhere to our guidelines," that "[e]very week, nearly 500 dedicated experts around the world review over 130k apps," and that "more than 1.9M app submissions were rejected for reasons that include privacy violations and fraudulent activity."[81]

159. As a result of these and other implied and express representations, including Apple's long-term advertising campaign regarding the safety of its apps as alleged above, Plaintiffs and Class members purchased iPhones and iPads and downloaded and used scam cryptocurrency trading apps (including Digicoins, SolLuna, Forex5, and Swiftcrypt apps) from the App Store. As a result of Apple's misconduct and representations, including its substantial assistance and participation in the pig butchering frauds perpetrated through the Apple App Store apps, Plaintiffs also lost thousands of dollars in scam apps they acquired through Apple's App Store.

[81] Apple, *App Store* (homepage), Apple.com, available at https://www.apple.com/app-store/ (last visited Aug. 21, 2025). *See also* Exhibit A attached (compendium of Apple's App Store homepage from 2020 to the present).

160. A reasonable consumer would be deceived or mislead by Apple's representations because the representations regarding the legitimacy, safety and security of App Store apps are material to consumers' decision to purchase iPhones and iPads and download and use App Store apps for financial transactions and purposes.

161. Notwithstanding these representations, the cryptocurrency trading applications on the App Store were not vetted, legitimate, safe and trustworthy and Defendant failed to properly vet cryptocurrency trading applications before providing them to the public.

162. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(2) of the CLRA by misrepresenting the source, sponsorship, approval, or certification of its goods or services.

163. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(5) of the CLRA by representing that its goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have.

164. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(7) of the CLRA by representing that its goods or services are of a particular standard, quality, or grade, when in fact, they are of another.

165. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(9) of the CLRA by advertising goods . . . with intent not to sell them as advertised.

166. Defendant's violations of the CLRA present a continuing threat to Plaintiffs and Class members in that Defendant continues to engage in the above-referenced acts and practices, and unless enjoined from doing so by this Court, will continue to do so. Plaintiffs own Apple products, including iPhones, and therefore intend to continue to download and use App Store apps in the future if they are secure and comport with Apple's claims regarding standards, vetting and review. Because Plaintiffs own Apple iPhones and/or iPads, and the ability to download and use apps is integral to the core functionality of the Apple devices they own, they have no reasonable, comparable alternatives except to download and use apps from Apple's App Store. If Apple is not

enjoined from continuing its unfair business practices in violation of the UCL, Plaintiffs will not know whether the App Store apps, and especially financial apps, are safe, vetted and legitimate and cannot safely use or download such apps in the future without subjecting themselves to other financial scams perpetrated via unvetted, scam App Store apps. Injunctive relief, in the form of corrective advertising, is necessary to dispel public misperception about the safety and trustworthiness of apps in Apple's App Store that has results from years of Apple's unlawful marketing efforts and to prevent current and future Apple product users from being misled. Defendant's conduct is fraudulent, wanton and malicious.

167. Plaintiffs seek an order awarding actual damages pursuant to Civil Code § 1780 (a)(1) for the actual damages they and Class members suffered as a result of Apple's violations of the CLRA, including the money Plaintiffs and Class members lost to the scam cryptocurrency apps, in an amount to be determined at trial.

168. Plaintiffs seek an order awarding restitution pursuant to Civil Code § 1780 (a)(3), including for the amount they overpaid for iPhones and other Apple products, which overpayments were received in whole or in part by Defendant, and for money taken from them as alleged, in an amount to be determined at trial.

169. Plaintiffs seek an order enjoining Apple pursuant to Civil Code § 1780 (a)(2) from its ongoing violations of the CLRA and ongoing failure to vet the safety, security and legitimacy of cryptocurrency trading apps available on the App Store which presents a continuing threat to Plaintiffs who are prohibited by Apple from downloading or using apps on their devices that are not from the App Store, while simultaneously not adequately vetting or ensuring the safety and legitimacy of App Store apps.

170. Plaintiffs seek an award of attorneys' fees and costs pursuant to Civil Code § 1780(e).

171. In compliance with Civil Code section 1782, more than 30 days before bringing these claims, Plaintiffs provided notice to Defendant of its violations and provided it with an opportunity to cure its violations. Defendant did not avail itself of this opportunity. Plaintiffs and the Class are therefore entitled to all forms of relief provided by the CLRA. In compliance with Civil Code section

1780(d), attached as Exhibit C is the affidavit showing that the action has been commenced in the proper forum.

COUNT III

Negligent Misrepresentation

172. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

173. Apple has represented for years that its App Store is a safe and trusted place to obtain apps for over a decade. This representation appears at the top of its website for the App Store. It touts its review of proposed apps, claiming that the company is "[d]edicated to trust and safety."

174. Despite its many representations to consumers that the App Store is safe and trusted, Apple approves fraudulent apps on the App Store which are solely designed to steal money from the users of the apps.

175. Apple knew, or should have known, that these types of apps exist on the App Store, yet still makes these representations to consumers. Apple knew, or should have known, that pig-butchering scams exist and, through reports from users of the App Store, knew, or should have known, that fraudsters were conducting these pig-butchering schemes through apps on the App Store.

176. Apple's misrepresentations regarding the App Store are material facts to consumers who use the App Store. This is demonstrated by Apple's dedication to Apple's marketing of the App Store as safe and trusted. Apple makes these representations with an intent to induce consumers to rely on these statements and use the App Store with confidence that they will not be harmed by fraudulent apps.

177. Plaintiffs and Class members justifiably relied on Apple's years-long representations regarding the App Store's safety. Apple has made the safety of the App Store its core marketing message regarding the App Store.

///

///

///

178. Plaintiffs have suffered injury in fact and lost money or property as a result of Defendant's negligent misrepresentations alleged herein. Because of the misrepresentations, Plaintiffs and members of the Class have suffered an injury in fact and have lost money and property, including, but not limited to, the expected utility and performance of their Apple iPhones and iPads, the purchase price of their Apple devices, and/or the difference between the price Class members paid and the actual worth of the hardware product had Apple disclosed the true nature of the representations at issue. As a result of Defendant's misconduct and representations, including Apple's substantial assistance and participation in the pig butchering frauds perpetrated through the Apple App Store apps, Plaintiffs also invested and lost thousands of dollars in scam apps they acquired through Apple's App Store.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for judgment against Defendant as follows:

A. For an Order certifying the Class;

B. For an Order declaring Defendant's conduct unlawful;

C. For preliminary and permanent injunctive relief prohibiting Defendant from committing in the future those violations of law herein alleged and for corrective advertising to inform users regarding Defendant's failure to comply with its vetting and review of App Store apps;

D. For damages and restitution to Plaintiffs and to the Class as permitted by law and equity under the laws alleged herein;

E. For pre- and post- judgment interest according to proof;

F. For costs of suit, including reasonable attorney fees, costs, and expenses under applicable provisions of law;

G. For all other relief this Court deems just, equitable, and proper.

///

///

///

///

JURY DEMAND

Plaintiffs hereby request a jury trial for all issues triable by jury.

Respectfully submitted,

Dated: August 28, 2025

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
LESLIE E. HURST (178432)
THOMAS J. O'REARDON II (247952)
ADAM M. BUCCI (327312)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
lhurst@bholaw.com
toreardon@bholaw.com
abucci@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW (*pro hac vice*)
ANTHONY L. PARKHILL (*pro hac vice*)
205 W. Randolph Street, #1630
Chicago, IL 60606
Tel: 312/621/2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on August 28, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail Notice List.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on August 28, 2025.

s/ Timothy G. Blood
TIMOTHY G. BLOOD